PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-208946

(43)Date of publication of application : 26.07.2002

(51)Int.Cl. H04L 12/56

(21)Application number : 2001-003436

(22)Date of filing : 11.01.2001

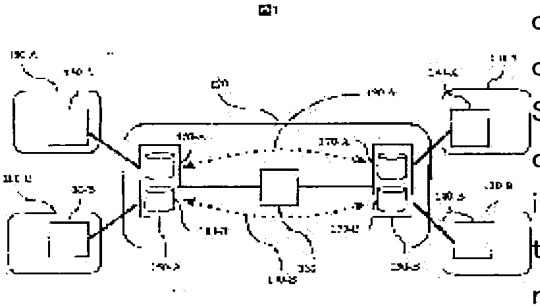
(71)Applicant : HITACHI LTD

(72)Inventor : NAKAYAMA MASAKI
TSUGE MUNETOSHI
KIMOTO ATSUSHI

(54) ROUTE INFORMATION NOTIFICATION METHOD AND VPN SERVICE AND EDGE ROUTER DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an IP-VPN service of a method for providing a VPN service at low costs by diverting an already existing technology by logically or physically multiplying the communication of a VPN user between the edge routers of a communication agent network.



SOLUTION: Edge routers 150-A and 150-B arranged in a communication agent network respectively store received route information in the route table of the corresponding VPN, and notify the other edge router of the route information by a route information notifying means independent for each VPN. The other edge router device which receives the route information selects the corresponding VPN, and stores the route information in the route table of the selected VPN. Thus, it is not necessary to extend any BGP protocol. Therefore, it is possible for a communication agent to utilize the already existing router, and to easily construct the VPN service.

CLAIMS

[Claim(s)]

[Claim 1]As opposed to two or more VPN user networks connected to at least one physical network, It is a channel information notifying method of VPN (Virtual Private Network) service which provides a virtual permanent communication way for every user, An edge router device which exists in a physical network network and is arranged at a contacting part with two or more above-mentioned VPN user networks, A channel information notifying method notifying channel information received from two or more above-mentioned VPN user networks to other edge router devices by a channel information reporting means which was able to be independently established for every VPN.

[Claim 2]In order that an edge router device besides the above may make selectable a VPN user corresponding to received channel information in claim 1, By using a transmission source address which is different when holding a conversion table of an IP address a transmitting agency edge router device's, and a VPN user's identifier and notifying channel information of different VPN, A channel information notifying method, wherein an edge router device besides the above chooses VPN corresponding to received channel information using the above-mentioned conversion table.

[Claim 3]In order that an edge router device besides the above may make selectable VPN corresponding to received channel information in claim 1, In setting-operation of a connection for the notice of a course on which the above-mentioned edge router device is performed in advance of a notice of channel information, A channel information notifying method, wherein recognition of VPN corresponding to channel information received henceforth of an edge router device besides the above is attained by including an identifier of VPN in a connection setting request message.

[Claim 4]As opposed to two or more VPN user networks connected to at least one physical network, It is a VPN service which provides a virtual permanent communication way for every user, A VPN service, wherein a channel information reporting means which exists in a physical network network and is arranged at a contacting part with two or more above-mentioned VPN user networks and which has two or more edge router devices, and became independent to two or more above-mentioned VPN user networks between the above-mentioned plurality edge router devices is established.

[Claim 5]As opposed to two or more VPN user networks connected to at least one physical network, It is an edge router device used for VPN (Virtual Private Network) service which provides a virtual permanent communication way for every user, The edge router device exists in a physical network network, and is arranged at a contacting part with two or more above-mentioned VPN user networks, An edge router device, wherein said the edge router device can notify channel information received from two or more above-mentioned VPN user networks to other edge router devices via a channel information reporting means which was able to be independently established for every VPN user.

[Claim 6]As opposed to two or more VPN user networks connected to at least one physical network, It is a channel information notifying method of VPN (Virtual Private Network) service which provides a virtual permanent communication way for every user, An edge router device which exists in a physical network network and is arranged at a contacting part with two or more above-mentioned VPN user networks, Have

the route table which became independent for every VPN, and the above-mentioned edge router device stores in a corresponding route table of VPN channel information received from two or more above-mentioned VPN user networks, and. A channel information notifying method notifying the above-mentioned channel information to other edge router devices by a channel information reporting means independently established for every VPN.
[Claim 7]A network system which has a network which connects two or more user networks characterized by comprising the following, and a user network of this plurality mutually.
A virtual permanent communication way for transmitting and receiving information among two or more above-mentioned user networks is set as the above-mentioned network, It is a method for notifying channel information for building VPN containing a user network of this plurality among two or more router devices which connect each of a user network of this plurality to this network, A step which sets up a channel corresponding to VPN by which the above-mentioned construction of [for notifying the above-mentioned channel information among two or more above-mentioned router devices] is carried out.
A step which notifies channel information of a user network contained in VPN corresponding to this channel via the above-mentioned channel.
[Claim 8]A channel information notifying method which is the channel information notifying method according to claim 7, and is characterized by a step which sets up said channel having a step which requires setting out of said channel using identification information of said VPN built.
[Claim 9]A channel information notifying method, wherein it is the channel information notifying method according to claim 8 and said identification information is an IP address corresponding to said VPN built.
[Claim 10]A router device characterized by comprising the following for connecting two or more user networks mutually, and connecting a user network to a network which builds VPN which sets up a virtual permanent communication way for transmission and reception of information between user networks of this plurality, and contains a user network of this plurality.
The first means of communication for communicating with a user network.
The second means of communication for communicating with other router devices linked to the above-mentioned network.
A user network which communicates via the first means of communication of the above.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]In the network system which is serving the virtual private network, this invention relates to the art for exchanging the course of a user network between edge routers.
[0002]
[Description of the Prior Art]By rapid progress of network technology, the computer in a its company building is connected in a company etc., and the demand of liking to use it in a building, connecting applications, such as WWW (World Wide Web) and mail, is increasing. It was widely realized by the spread of LAN (Local Area Network) which connects the computer in a building mutually. Next, it changed to

connecting each branch office by which users' demand is distributed locally and LAN maintenance is carried out. The virtual private network (VPN) which can use the network in the private state virtually at the user side attracts attention by providing the network which connects the company user of the position from which a net provider differs as art of realizing it. How to multiplex a VPN customer's communication logically or physically can be considered between the edge routers placed by the edge part of the communication enterprise network, i.e., the peripheral part which is points of contact with a customer network, as a method of building VPN among the user hosts who are in a remote place mutually. Thereby, from a VPN customer, it is visible as connected in the dedicated line. In this method, since a customer network and a communication enterprise network can use an Internet protocol address, IP-VPN service of VPN of this method is written below.

[0003]The art of realizing IP-VPN is indicated by RFC2547 which is a standard document which standardization organization IETF (Internet Engineering Task Force) of Internet technique specifies. By RFC2547, in order to build IP-VPN service, carrying out the following processings to the edge router of a communication enterprise is described. An edge router holds and manages first the route table separated for every VPN site. And the course of a route table is exchanged using BGP which is a routing protocol between edge routers. Since it specifies in which route table in the edge router of a report destination the course to notify is written when notifying a course to other edge routers from an edge router, the following extended mounting has been given to the edge router. it is a set of the IP address belonging to a certain group -- the prefix of the course equivalent to the group of an IP address and a subnet mask (length from the starting point of an IP address to a terminal point) -- in addition, It adds to the course message which notifies the identifier which specifies in which route table the course is written by BGP, and the edge router of the course receipt point writes it in the route table for every VPN site managed by itself, seeing the identifier. He is a BGP peer (.) so that in other words it may be shown concretely at drawing 18. Namely, course exchange reporting means 190-A for two sets of the routers which had the BGP protocol mounted is stretched between [one] the edge routers 150, In order to use in common by two or more VPN user network 100-A, 100-B, 110-A, and 110-B, it will be necessary to add the VPN identifier used for a course notification message by a data communication line. In drawing 18, one tunnel (data communication line) 195 is further formed as an object for data packet transmission between the edge routers 150. These BGP peer and a tunnel function mutually independently.

[0004]

[Problem(s) to be Solved by the Invention]There are the following two problems in the conventional technology at the time of offering IP-VPN service.

[0005]The first problem is extending a BGP protocol in order to add the identifier of a route table to the course notification message of BGP. For this reason, interconnection with the router designed based on the existing BGP protocol becomes impossible. The second problem is being unable to divert the existing filtering function, when realizing course filtering functions, such as incorporation point specification (selection of the route table to reflect), to the channel information of each which the edge router received. In the existing BGP protocol without the concept of VPN, following three existed in the course filtering function. The 1st is the BGP peer unit used for course transmission and reception, and it is a filter which can choose whether the course which went via the peer (channel) is stored or discarded. It is a prefix unit

which is a group of the 2nd, an IP address, and a subnet mask, and is a filter which can choose whether a course is stored or discarded. The 3rd is a form where the two above-mentioned filters were set, they are a group of the BGP peer for course transmission, and an IP address, and are a filter which can choose whether a course is stored or discarded.

[0006]However, since filtering using the VPN identifier added to the course notification message cannot be performed, a route table is inseparable in these functions, for every VPN site using the existing filter.

[0007]When it is going to provide a VPN service, these problems mean that the software update of all the edge routers virtual private within the net or device exchange is needed, and lead to introduction cost going up remarkably.

[0008]

[Means for Solving the Problem]In this invention, an edge router is installed within the net [of a communication enterprise], and it is connected by a router and a circuit of a VPN customer network. An edge router of a communication enterprise receives a course of a VPN site in which it is installed, from a router of a VPN customer network.

[0009]An edge router of a communication enterprise notifies a received course to other edge routers of a communication enterprise using a routing protocol. Other edge routers which received a course recognize VPN corresponding to the course by a method shown below, and write a course in a route table corresponding to recognized VPN, and they notify the course to a router of a connected user network.

[0010]It is exchanged in a course of a user network by the above.

[0011]When an edge router of a communication enterprise receives a VPN customer's course, how to identify the VPN is shown. A VPN identifier is not included in a course notification message called a UPDATE message (a path attribute to course deletion / addition, and an IP address is comprised) which is a packet of channel information in this invention, VPN is identified using a connection request message required as stretching a peer of BGP for transmitting and receiving a course notification message between edge routers.

[0012]A method of identifying VPN by a connection request message has two of the followings.

[0013]A primary method identifies VPN by a connection partner's IP address included in a connection request message, when an edge router receives a connection request message. By referring to an IP address of a connection partner who had registered by an administrator of an edge router beforehand, and a conversion table of a VPN identifier, matching with a connection request message and a VPN identifier is attained. The second method is adding a VPN identifier to a message of a connection request, when an edge router's transmits a connection request message, and an edge router of a side which receives a connection request discriminates VPN from a connection request message. A connection request message is also called an OPEN message and comprises a BGP header (BGP-ID which is an informer address is comprised), and an IP header (IP address which shows a transmitting agency / transmission destination). By this method, a VPN identifier in a request message can be compared with a VPN identifier which is in its configuration definition immediately in an edge router of a side which received a connection request.

[0014]An edge router will stretch a BGP peer for transmitting and receiving a course notification message about the VPN, if VPN is discriminated from a connection request message.

[0015]Therefore, the edge router can identify the thing corresponding to which VPN a course notification

message transmitted and received via the BGP peer for every BGP peer is.

[0016]A VPN customer's course can be exchanged between edge routers, without this extending a course notification message. Since a BGP peer is prepared for a VPN user unit by this method also about a course filter, a filter of the existing BGP peer unit can be diverted as a filter of a VPN user unit as it is. As opposed to a specific user by whom this invention is furthermore connected to one physical network, It is a VPN service to two or more VPN users who provide a virtual permanent communication way for every user, Exist in a physical network network and it has a plurality edge router device arranged at a contacting part with a user network, Each edge router device is providing a VPN service, wherein it has a route table relevant to a VPN user and two or more channel information reporting means which became independent to two or more VPN users at least are established between edge router devices. As opposed to a specific user by whom this invention is furthermore connected to one physical network, It is an edge router device used for a VPN service which provides a virtual permanent communication way for every user, The edge router device exists in a physical network network, and is arranged at a contacting part with a user network, [two or more] It is providing an edge router device, wherein each edge router device's has a route table relevant to a VPN user and a channel information reporting means which became independent for every VPN user may be established among two or more edge router devices.

[0017]A network system which furthermore has a network which connects mutually two or more user networks which are characterized by that that this invention provides a channel information notifying method comprises the following, and a user network of this plurality.

A virtual permanent communication way for transmitting and receiving information among two or more above-mentioned user networks is set as the above-mentioned network, It is a method for notifying channel information for building VPN containing a user network of this plurality among two or more router devices which connect each of a user network of this plurality to this network, A step which sets up a channel corresponding to VPN by which the above-mentioned construction of [for notifying the above-mentioned channel information among two or more above-mentioned router devices] is carried out.

A step which notifies channel information of a user network contained in VPN corresponding to this channel via the above-mentioned channel.

[0018]In the above-mentioned channel information notifying method, a step which sets up said channel has a step which requires setting out of said channel using identification information of said VPN built.

[0019]In the above-mentioned channel information notifying method, said identification information is characterized by being an IP address corresponding to said VPN built.

[0020]Furthermore, this invention connects two or more user networks mutually, and a virtual permanent communication way for transmission and reception of information between user networks of this plurality is set up, The first means of communication for being a router device for connecting a user network to a network which builds VPN containing a user network of this plurality, and communicating with a user network, In order to build VPN containing a user network which communicates via the second means of communication and first means of communication of the above for communicating with other router devices linked to the above-mentioned network, It has a channel management tool which manages a channel for transmitting and receiving channel information of a user network contained in this VPN among other router devices which communicate via the second means of communication of the above, Match the

above-mentioned channel management tool with VPN built, manage the above-mentioned channel, and the second means of communication of the above, When transmitting or receiving channel information for building VPN, the above-mentioned channel management tool is providing a router device using a channel which was matched with VPN this built and has been managed.

[0021]

[Embodiment of the Invention]Hereafter, this invention is explained using a drawing.

[0022]Drawing 1 shows the system configuration of VPN. This system comprises the communication enterprise network 120, user network 100-A, 100-B, 110-A, and 110-B. 100-A and 110-A use a certain user network, 100-B, and 110-B as another user network. From 100-A, it can communicate normally on a communication enterprise network to 110-A. Since the communication to 100-B from 100-A or 110-B differs in a user, it covers communication. When user networks differ, address spaces also differ. For example, the IP address currently used with a certain user network can also be used with other user networks.

[0023]The route table 160 or 170 in the edge router 150 is managed for every VPN. Route table 160-A in edge router 150-A receives the course in user network 100-A corresponding to a route table from router 130-A of a user network, and writes it in. And the course notified from route table 170-A in another edge router 150-B which belongs to the same VPN is also written in. It is necessary to prepare the course exchange reporting means which became independent for every VPN as pre-preparation of exchange of the VPN course between the edge routers 150. There is a peer of a BGP protocol as an example of a course exchange reporting means. In practice, it is the thing of TCP (Transfer Control Protocol) connection to which communication was guaranteed on the IP network, and is exchanged in a course using the TCP connection. Subsequent explanation explains a course exchange reporting means using the term of a BGP peer.

[0024]BGP peer 190-A and 190-B are prepared for every VPN. The information which identifies VPN is not included in the route notifying packet which flows on a BGP peer. The edge router which received channel information specifies VPN of the notified course with reference to the BGP peer management table 346 (it explains in full detail in drawing 5) which is a conversion table of a BGP peer and a VPN identifier.

[0025]A channel is set up between the edge routers 150 and communication between VPN sites is performed by passing the data packet of VPN to the channel. The core router 180 does not hold the route table of VPN, but relays the data packet of VPN using the set-up channel.

[0026]Drawing 2 shows the hardware constitutions of the edge router 150.

[0027]CPU(Central Processing Unit) 200 is a processor for executing the program stored in the memory 210. In the memory 210, the control program 215 for performing the operating system 213 for controlling the whole device and operation as a router device is stored.

[0028]The user network side network controller 220 controls the transmission and reception which the edge router 150 performs between the routers of a user network. The communication enterprise network side network controller 225 controls the transmission and reception which the edge router 150 performs between a partner's edge routers 150. The keyboard controller 230 controls the keystroke from the keyboard 235. The serial controller 240 controls input/output devices, such as the mouse 245 connected to the serial port. The controller displays 250 control a screen display to the display monitor 255. The disk

controller 260 controls the input and output to the disk unit 265.

[0029]Although premised on performing operation of the edge router 150 by a network administrator in this example from the keyboard 235, the mouse 245, and the display monitor 255 by which direct continuation was carried out to the device, Of course, it is also possible to operate it using the input/output device in the remote place connected via the edge router 150 and the network.

[0030]Drawing 3 shows the software configuration of the edge router 150.

[0031]I/O control unit 310 controls the input from a keyboard, and the output to a display.

[0032]The user network side network interface part 380 performs processing about transmission and reception between the routers by the side of a user network, such as passing the user network side communications department 360 the packet which received from the router by the side of a user network, or transmitting a packet to a network by demand of the user network side communications department 360.

[0033]The communication enterprise network side network interface part 390, Processing about transmission and reception between the edge routers 150 by the side of a communication enterprise network, such as passing the communication enterprise network side communications department 370 the packet which received from the edge router 150 by the side of other communication enterprise networks, or transmitting a packet to a network by demand of the communication enterprise network side communications department 370, is performed.

[0034]The user network side communications department 360 the packet which received from the user network side network interface part 380, According to the result, pass the direction of the suitable treatment module of the routing protocol packet analyzing parts 340 and the data relay parts 350, or, Packet distribution processing to the interpretation and each module of a packet header according to an internal protocol, such as adding the suitable header for the packet passed from these treatment modules, and passing the user network side network interface part 380, is performed. This user network side communications department 360 is taken as the first means of communication for communicating with a user network here.

[0035]The communication enterprise network side communications department 370 the packet which received from the communication enterprise network side network interface part 390, According to the result, pass the direction of the suitable treatment module of the routing protocol packet analyzing parts 340 and the data relay parts 350, or, Packet distribution processing to the interpretation and each module of a packet header according to an internal protocol, such as adding the suitable header for the packet passed from these treatment modules, and passing the communication enterprise network side network interface part 390, is performed. This communication enterprise network side communications department 370 is taken as the second means of communication for communicating with other edge router devices linked to a network here.

[0036]The data relay part 350 relays the data of the user network side communications department 360, the communication enterprise network side communications department 370, and the routing protocol packet analyzing parts 340, and determines to which functional block it transmits with reference to the header of a packet. Furthermore, in the case of data transfer, the interface to send out is determined with reference to the route table 160 or 170.

[0037]After analyzing the packet of a routing protocol, the routing protocol packet analyzing parts 340 pass

the course filter Management Department 330 channel information, in order to add or delete a course. If the connection request packet of BGP is normal, connection is requested from the BGP peer Management Department 344 in order to register it.

[0038]The BGP peer Management Department 344 holds the connection, when connection of BGP is successful. In order that this BGP peer Management Department 344 may build here VPN containing the user network which communicates via the first means of communication of the above, It is considered as the channel management tool which manages the channel for transmitting and receiving the channel information of the user network contained in this VPN among other edge router devices which communicate via the second means of communication of the above. An initial entry is written in the BGP peer management table 346.

[0039]The course filter Management Department 330 decides with reference to the course filter table 335 which restricts the addition of a course whether to permit it, when there is an addition of a course or a demand of deletion by the routing protocol packet analyzing parts 340.

[0040]Since the route table Management Department 320 writes the course permitted with the course filter in the route table 160 or 170 managed for every VPN and each route table supports VPN, With reference to the BGP peer management table 346, it is specified as which VPN whether a course is written in. The route table Management Department 320 searches the route table 160 or 170 for data packet transmission.

[0041]Drawing 4 shows the form of the route table 160 or 170 which the edge router 150 uses. It dissociates for every VPN and this route table is held within a router.

[0042]The channel information of each VPN is stored in the route table 160 or 170 by table format. The inside of the IP address constituted from IP address 410, network ID, and host ID of a course by each channel information, The subnet mask 420 used since the length of network ID is specified, NextHop430, the interface identifier 440, IP address 450 of a course transmitting former router, and the attribute 460 of a course are contained.

[0043]IP address 410 of a course, the subnet mask 420, and NextHop430 are notified from other routers. In order that NextHop430 may reach the transmitting agency router which notified the course, the edge router 150 shows the address of the following router to which a data packet is transmitted. The interface identifier 440 is an identifier for specifying the interface by the side of the edge router 150 connected to NextHop430.

[0044]IP address 450 of a course transmitting former router identifies the BGP peer of course transmitting origin. The IP address of a course transmitting former router is used for a course filter. For example, when it corresponds to setting out of the administrator of not writing all the courses that came from a certain BGP peer in the route table 160 or 170, IP address 450 of the course transmitting former router whether the course was notified by which BGP peer is referred to.

[0045]The attribute 460 of the course is prescribed by the BGP protocol. For example, when the same course is notified by two or more BGP peers, the cost of the course which course to adopt is specified.

[0046]Drawing 5 shows the form of the BGP peer management table 346 which an edge router uses.

[0047]The BGP peer identifier 510, a connection partner's IP address 520, and VPN-ID530 are contained in the BGP peer management table 346 of drawing 5. The BGP peer identifier 510 is a number which identifies the BGP peer who holds within this device. When the connection request of BGP is received, since VPN of the connection is specified, a connection partner's IP address 520 and VPN-ID530 are used.

[0048]A connection request is processing required of the edge router of these others as stretching a BGP peer, in order that an edge router may perform course exchange among other edge routers, and an edge router notifies the information on a self-edge router to the edge router of these others, in order to obtain permission of course exchange. A connection-request receiver router accepts connection to the transmitting side, or chooses either which is accepted and twisted, and returns the reply to the connection-request side router. The router which was able to accept the connection request can stretch a BGP peer, and can notify a course using a BGP peer according to a BGP protocol. In two sets of the BGP routers with which the BGP peer was stretched, it is automatically exchanged in channel information.
[0049]Drawing 6 is a sequence which shows exchange of the VPN course between the edge routers 150 after VPN course registration of the edge router 150, and registration. The administrator of the edge router A performs setting out which connects the BGP peer for course exchange with the router of a user network first (sequence 610-A). The same of the setting out may be said of the case of the edge router B (sequence 610-B), and the setting order of the edge router A and the edge router B is not asked.
[0050]The edge router A which received a BGP peer's setting out advances the connection request of the peer for course exchange from an administrator to the router A of a user network (sequence 620-A). The router A of the user network which received the connection request returns ACK, when accepting a connection request, and when refusing, it returns NOTIFY which is an error notification (sequence 630-A). The edge router A transmits a connection request message, in order to connect the BGP peer for course exchange to B which is other edge routers of a communication enterprise network (sequence 640). The edge router B which received the connection request message returns ACK, when accepting a demand, and when that is not right, it returns NOTIFY (sequence 650). After a user network and communication enterprise network side's connecting a BGP peer to both by the above, a course is notified to the edge router A from the router A of a user network. The edge router A which received the notice writes the course in the route table for every VPN user held in a router, exists in a communication enterprise network, and also it notifies the course to B which is an edge router (sequence 660-A). The edge router B notifies a VPN course to the edge router A similarly (sequence 660-B).
[0051]Drawing 7 is a sequence which shows VPN deletion of the edge router A. The case where a certain user network is deleted with the edge router A is shown.
[0052]The administrator of the edge router A sets up deletion of the BGP peer beforehand stuck on the user network A to the edge router A (sequence 710). The edge router A which received the command of BGP peer deletion advances a BGP peer's deletion request to the router A of a user network (sequence 720). After the router A of the user network which received the deletion request checks whether the deletion request can operate normally, it permits deletion or returns an error (sequence 730). Since the router A and the edge router A of a user network hold the course notified from the edge router B for every BGP peer, all the courses notified by the BGP peer are deleted from the route table in the router A of a user network with deletion of the BGP peer stuck between the edge routers A.
[0053]The edge router A which received the deletion response from the router A of a user network advances a BGP peer's deletion request to the edge router B (sequence 740). The edge router B which received the peer's deletion request deletes a peer with a deletion request from the BGP peer management table in a router, and returns ACK (sequence 750). The course notified to the edge router B from the edge

router A before a BGP peer's deletion is deleted from the route table for every VPN at the time of a peer's deletion.

[0054]Drawing 8 is a sequence which shows VPN deletion with the edge router A and the edge router B.

[0055]The administrator of the edge router A sets up deletion of the BGP peer beforehand stuck on the user network A to the edge router A (sequence 810-A). The administrator of the edge router B also sets up deletion of the BGP peer beforehand stuck on the user network B to the edge router B in a similar manner (sequence 810-B).

[0056]The edge router A which received the command of BGP peer deletion advances a BGP peer's deletion request to the router A of a user network (sequence 820-A). The edge router B with which communication enterprise network router device B received the command of BGP peer deletion similarly advances a BGP peer's deletion request to the router B of a user network (sequence 820-B). After the router A of the user network which received the deletion request checks whether the deletion request can operate normally, it permits deletion or returns an error (sequence 830-A). After the router B of the user network with which the user network router B side received the deletion request similarly checks whether the deletion request can operate normally, it permits deletion or returns an error (sequence 830-B).

[0057]After the BGP peer deletion by the side of the user network routers A and B is completed, the edge routers A and B perform BGP peer deletion between edge routers (sequences 840 and 850).

[0058]Drawing 9 is a sequence of the data communications between user networks. The edge routers A and B should finish exchanging the course of the user network as pre-preparation of data communications. The sequence which communicates a data packet is shown in the router B of a user network from the router A of a user network.

[0059]The router A of a user network transmits a data packet to the edge router A (sequence 910). The edge router A which received the data packet transmits a data packet to the edge router B with reference to the route table corresponding to VPN of a data packet (sequence 920). The edge router B receives a data packet and transmits a data packet to the router B of a user network with reference to the route table corresponding to VPN of a data packet (sequence 930).

[0060]Drawing 10 is a BGP peer connection-request flow with the router of a user network of the edge router 150. The edge router 150 into which the connection request was inputted from the network administrator (Step 1005) transmits to the router of a user network with the IP address specified in the connection request message of the BGP protocol (Step 1010). The edge router 150 waits for ACK of connection from the router of a user network after that. When the router of a user network refuses the connection request of the edge router 150 for the reasons of an error etc., the router of a user network returns NOTIFY which is an error message to the edge router 150 (Step 1020). If not ACK but NOTIFY is received, an error will be outputted to a display monitor (Step 1025). If ACK which shows that the BGP peer was normally connected from the connection partner is received (Step 1030), the BGP peer information that it succeeded in connection will be added to the BGP peer management table 346 (Step 1040).

Drawing 11 is a receiving flow of the BGP peer connection request from the router of a user network of the edge router 150.

[0061]Before receiving a connection request message, the edge router 150 inputs the IP address of the partner router which permits connection (Step 1105). Setting out which enumerates one IP address at a

time, and setting out which permits all the IP addresses by the side of a connection request are performed. A connection request message is received from a connection partner router after that (Step 1110). The receiver edge router 150 which received the connection request message checks a connection request message. Discover abnormalities to a connection-request message packet, or (Step 1120), When the request message from the connection partner who has not set it as the IP address of the partner who permits the above-mentioned connection arrives (Step 1130), Connection is not established, but NOTIFY which is an error message is transmitted to a connection-request former router (Step 1125), and an error is outputted to a display monitor (Step 1135).

[0062]When it permits connection, ACK is replied to a connection partner (Step 1140) and the connection-request receiver edge router 150 registers a new BGP peer into the BGP peer management table 346 in a router. Drawing 12 shows the flow of the connection-request processing of the edge router 150 at the time of making BGP peer connection between the edge routers 150.

[0063]It is shown on the assumption that the method which adds VPN-ID to a connection request message clearly as a method of identifying a BGP peer's VPN. A network administrator sets the IP address and VPN-ID of a BGP peer connection destination as the edge router 150 in a group (Step 1205). The edge router 150 which received setting out from an administrator transmits a connection request message with VPN-ID to a connection partner's edge router 150 (Step 1210). It waits for connection ACK after that. When a connection partner's edge router 150 refuses connection, NOTIFY which shows an error and its cause is returned to the edge router 150 by the side of a connection request (Step 1220). The edge router 150 which received NOTIFY outputs an error to a display monitor in order to notify an administrator of it (Step 1225). When a BGP peer's connection is normally permitted from a connection partner's edge router 150, the edge router which transmitted the connection request receives ACK (Step 1230). The edge router 150 which received ACK adds the BGP peer who newly connects to the management table 346 (Step 1240).

[0064]Drawing 13 shows the flow of the connection receiver processing of the edge router 150 at the time of making BGP peer connection between the edge routers 150. It is shown on the assumption that the method which adds VPN-ID to a connection request message clearly as a method of identifying a BGP peer's VPN. A network administrator registers the IP address of the partner who permits connection, before receiving a connection request message from the other edge routers 150 (Step 1305). A connection request message is received after that (Step 1310), and the connection request message which received is checked. As for the case that the value of VPN-ID which is not in agreement with the IP address of the partner who abnormalities are discovered by the connection-request message packet, or permits (Step 1320) and connection (Step 1330) and which is contained in a connection request message is unusual (Step 1340) etc., connection is refused. In order to transmit NOTIFY in order to notify an error to the edge router 150 of connection-request origin (Step 1325), and to notify a router administrator, an error is outputted to a display monitor (Step 1335). ACK is replied to the connection-request side when accepting a connection request (Step 1350). In order to register new connection, it adds to the BGP peer management table 346 (Step 1360).

[0065]Drawing 14 shows the flow of the connection-request processing of the edge router 150 at the time of making BGP peer connection between the edge routers 150. The edge router 150 which received the connection request as a method of identifying a BGP peer's VPN shows on the assumption that the method

to which VPN-ID is made to correspond, a connection partner's IP address, and.

[0066]A network administrator sets the IP address and VPN-ID of a BGP peer connection destination as the edge router 150 in a group (Step 1405). The edge router 150 which received setting out from an administrator transmits a connection request message to a connection partner's edge router 150 (Step 1410). It waits for connection ACK after that. When a connection partner's edge router 150 refuses connection, NOTIFY which shows an error and its cause is returned to the edge router 150 by the side of a connection request (Step 1420). The edge router 150 which received NOTIFY outputs an error to a display monitor in order to notify an administrator of it (Step 1425). When a BGP peer's connection is normally permitted from a connection partner's edge router 150, the edge router 150 which transmitted the connection request receives ACK (Step 1430). The edge router 150 which received ACK adds the BGP peer who newly connects to the management table 346 (Step 1440).

[0067]Drawing 15 shows the flow of the connection receiver processing of the edge router 150 at the time of making BGP peer connection between the edge routers 150. The edge router 150 which received the connection request as a method of identifying a BGP peer's VPN shows on the assumption that the method to which VPN-ID is made to correspond, a connection partner's IP address, and. A network administrator registers the IP address of the partner who permits connection, and corresponding VPN-ID, before receiving a connection request message from the other edge routers 150 (Step 1505). A connection request message is received after that (Step 1510), and the connection request message which received is checked. Connection is refused when not in agreement with the IP address of the partner who abnormalities are discovered by the connection-request message packet, or permits (Step 1520) and connection (Step 1530). In order to transmit NOTIFY in order to notify an error to the edge router of connection-request origin (Step 1525), and to notify a network administrator, an error is outputted to a display monitor (Step 1535). When accepting a connection request, VPN-ID is specified from a connection partner's IP address (Step 1540). And ACK is replied to the connection-request side (Step 1550). In order to register new connection, it adds to the BGP peer management table 346 (Step 1560).

[0068]In a BGP peer's deletion in the edge router 150, drawing 16 shows the flow by the side of a deletion request. A network administrator inputs the IP address of the BGP peer who deletes first (Step 1605). Next, a deletion request message is transmitted to a BGP peer partner's edge router 150 (Step 1610). It waits for ACK from a connection deletion partner's edge router 150 after that.

[0069]If deletion goes wrong with a partner's edge router, the NOTIFY message which is an error notification will be replied (Step 1620). In that case, in order to notify a network administrator of an error, an error is outputted to a display monitor (Step 1625). If a partner's edge router 150 deletes a BGP peer normally, ACK which notifies it is replied (Step 1630). The edge router 150 deletes the entry of the peer who deleted from the BGP peer management table 346 after receiving ACK (Step 1640).

[0070]In a BGP peer's deletion in the edge router 150, drawing 17 shows the flow of a deletion request receiver. The edge router 150 receives a deletion request message (Step 1710). When the BGP peer who abnormalities existed in the connection request message, or was specified as (Step 1720) and the BGP peer management table 346 by the deletion message does not exist, NOTIFY which is an error message is transmitted and an error output is carried out to a display. When deletion is performed normally, ACK is replied to the other party edge router which transmitted the deletion request (Step 1740), and a BGP peer

applicable from the BGP peer management table 346 is deleted (Step 1750). Although the example was given by making into a communication enterprise the administrator of a physical network who provides a VPN service above, it is clear that it can divert also to a corporate network.

[0071]

[Effect of the Invention]By using the method described above, it enables a communication enterprise to build a VPN service easily using the existing router.

[0072]Therefore, since the existing setting-out knowledge can be diverted while introduction cost in case a communication enterprise is going to provide a VPN service becomes cheap, operation management cost also becomes cheap and a cheap VPN service can be provided for a user.

[Brief Description of the Drawings]

[Drawing 1]It is a lineblock diagram of the network system in the VPN service of this invention.

[Drawing 2]It is a hardware-constitutions figure of the edge router of this invention.

[Drawing 3]It is a software configuration figure of the edge router of this invention.

[Drawing 4]It is a figure showing the route table which an edge router uses.

[Drawing 5]It is a figure showing the BGP peer management table which an edge router uses.

[Drawing 6]It is a figure showing the sequence diagram in the case of the VPN registration between edge routers.

[Drawing 7]It is a sequence diagram in the case of VPN deletion with edge router of one of the two.

[Drawing 8]It is a sequence diagram in the case of VPN deletion with both edge routers.

[Drawing 9]It is a sequence diagram of the VPN communication between the routers of a user network.

[Drawing 10]It is a figure showing the flow of the BGP peer connection request by the side of a user network.

[Drawing 11]It is a figure showing the flow of the BGP peer connection reception by the side of a user network.

[Drawing 12]It is a figure showing the flow of the BGP peer connection request by the side of the communication enterprise of a method which includes a VPN identifier in a request message.

[Drawing 13]It is a figure showing the flow of the BGP peer connection reception by the side of the communication enterprise of a method which includes a VPN identifier in a request message.

[Drawing 14]It is a figure showing the flow of the BGP peer connection request by the side of the communication enterprise of a method which identifies VPN in a connection partner's address.

[Drawing 15]It is a figure showing the flow of the BGP peer connection reception by the side of the communication enterprise of a method which identifies VPN in a connection partner's address.

[Drawing 16]It is a figure showing the flow of the BGP peer deletion request by the side of a communication enterprise.

[Drawing 17]It is a figure showing the flow of the BGP peer deletion reception by the side of a communication enterprise.

[Drawing 18]It is a lineblock diagram of the network system in the conventional VPN service.

[Description of Notations]

100-A, 100-B, 110-A, 110-B -- The network of a user network, 120 -- The network of a communication enterprise network, 130-A, 130-B, 140-A, 140-B -- The router of a user network, 150-A, 150-B -- Edge

router, 160-A, 160-B, 170-A, 170-B -- Route table, 180 -- A core router, 190-A, a 190-B--BGP peer, 195 -- Tunnel, 200 -- CPU, 210 -- A memory, 213 -- Operating system, 215 -- Control software, 220 -- User network side network controller, 225 -- The communication enterprise network side network controller, 230 -- Keyboard controller, 235 -- A keyboard, 240 -- A serial controller, 245 -- Mouse, 250 -- Controller displays, 255 -- A display, 260 -- Disk controller, 265 -- A disk unit, 310 -- An I/O control unit, 320 -- Route table Management Department, 330 [-- The BGP peer Management Department, 346 / -- A BGP peer management table, 350 / -- A data relay part, 360 / -- User network side communications department,] -- The course filter Management Department, 335 -- A course filter table, 340 -- Routing protocol packet analyzing parts, 344 370 -- The communication enterprise network side communications department, 380 -- User network side network interface section, 390 -- A communication enterprise network network interface section, 410 -- The IP address of a course, 420 [-- The IP address of a course transmitting former router, 460 / -- The attribute of a course, 510 / -- A BGP peer identifier, 520 / -- A connection partner's IP address, 530 / -- VPN-ID.] -- The subnet mask of a course, 430 -- NextHop of a course, 440 -- An I/F identifier, 450

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－208946
（P2002－208946A）
(43)公開日　平成14年７月26日(2002.7.26)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/56	１００	Ｈ０４Ｌ　12/56	１００Ｚ　５Ｋ０３０

審査請求　未請求　請求項の数10　ＯＬ　（全 21 頁）

(21)出願番号　特願2001－3436(P2001－3436)

(22)出願日　平成13年１月11日(2001.1.11)

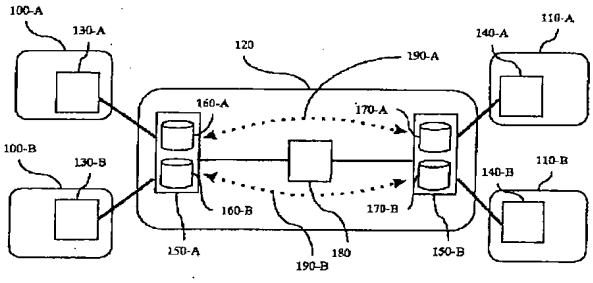
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　中山　正樹
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　柘植　宗俊
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100068504
弁理士　小川　勝男　（外２名）

最終頁に続く

(54)【発明の名称】　経路情報通知方法、ＶＰＮサービス及びエッジルータ装置

(57)【要約】
【課題】　通信事業者網のエッジルータ間で、ＶＰＮユーザの通信を論理的または物理的に多重化し、ＶＰＮサービスを提供する方法であるＩＰ－ＶＰＮサービスを既存技術を流用して安価に提供する。
【解決手段】　通信事業者網に配置されるエッジルータ１５０－Ａ、１５０－Ｂが、受信した経路情報を、対応するＶＰＮの経路テーブルに格納し、ＶＰＮ毎に独立した経路情報通知手段によって他のエッジルータに上記経路情報を通知し、受信した他のエッジルータ装置は、対応するＶＰＮを選択し、選択されたＶＰＮの経路テーブルに上記経路情報を格納する。
【効果】　ＢＧＰプロトコルの拡張が必要無いため、通信事業者が既存ルータを活用でき、ＶＰＮサービスを容易に構築することが可能となる。

図1



1

【特許請求の範囲】

【請求項１】少なくとも１つの物理ネットワークに接続される複数のＶＰＮユーザ網に対して、仮想的な専用通信路をユーザ毎に提供するＶＰＮ(Virtual Private Network)サービスの経路情報通知方法であって、物理ネットワーク網に存在し、上記複数のＶＰＮユーザ網との接点部分に配置されるエッジルータ装置が、上記複数のＶＰＮユーザ網から受信した経路情報をＶＰＮ毎に独立して設けられた経路情報通知手段によって他のエッジルータ装置に通知することを特徴とする経路情報通知方法。

【請求項２】請求項１において、上記他のエッジルータ装置が、受信した経路情報に対応するＶＰＮユーザを選択可能とするために、送信元エッジルータ装置のＩＰアドレスとＶＰＮユーザの識別子との対応表を保持し、異なるＶＰＮの経路情報を通知する際には異なる送信元アドレスを用いることにより、上記他のエッジルータ装置が、上記対応表を用いて、受信した経路情報に対応するＶＰＮを選択することを特徴とする経路情報通知方法。

【請求項３】請求項１において、上記他のエッジルータ装置が、受信した経路情報に対応するＶＰＮを選択可能とするために、上記エッジルータ装置が、経路情報通知に先立って行われる経路通知用コネクションの設定動作において、コネクション設定要求メッセージの中にＶＰＮの識別子を含ませることにより、上記他のエッジルータ装置が、以降受信する経路情報に対応するＶＰＮを認識可能となることを特徴とする経路情報通知方法。

【請求項４】少なくとも１つの物理ネットワークに接続される複数のＶＰＮユーザ網に対して、仮想的な専用通信路をユーザ毎に提供するＶＰＮサービスであって、物理ネットワーク網に存在し、上記複数のＶＰＮユーザ網との接点部分に配置される複数個エッジルータ装置を有し、上記複数個エッジルータ装置間には上記複数のＶＰＮユーザ網に対して独立した経路情報通知手段が設けられていることを特徴とするＶＰＮサービス。

【請求項５】少なくとも１つの物理ネットワークに接続される複数のＶＰＮユーザ網に対して、仮想的な専用通信路をユーザ毎に提供するＶＰＮ(Virtual Private Network)サービスに用いられるエッジルータ装置であって、そのエッジルータ装置は物理ネットワーク網に存在し、上記複数のＶＰＮユーザ網との接点部分に配置され、前記そのエッジルータ装置は上記複数のＶＰＮユーザ網から受信した経路情報をＶＰＮユーザ毎に独立して設けられた経路情報通知手段を介して他のエッジルータ装置に通知出来ることを特徴とするエッジルータ装置。

【請求項６】少なくとも１つの物理ネットワークに接続される複数のＶＰＮユーザ網に対して、仮想的な専用通信路をユーザ毎に提供するＶＰＮ(Virtual Private Network)サービスの経路情報通知方法であって、物理ネットワーク網に存在し、上記複数のＶＰＮユーザ網との接点部分に配置されるエッジルータ装置が、各ＶＰＮ毎に独立した経路テーブルを有し、上記エッジルータ装置は上記複数のＶＰＮユーザ網から受信した経路情報を、対応するＶＰＮの経路テーブルに格納すると共に、ＶＰＮ毎に独立して設けられた経路情報通知手段によって他のエッジルータ装置に上記経路情報を通知することを特徴とする経路情報通知方法。

2

【請求項７】複数のユーザ網と、該複数のユーザ網を相互に接続するネットワークとを有するネットワークシステムにおいて、上記複数のユーザ網間で情報の送受信を行うための仮想的な専用通信路を上記ネットワークに設定して、該複数のユーザ網を含むＶＰＮを構築するための経路情報を、該複数のユーザ網の各々を該ネットワークに接続する複数のルータ装置間で通知するための方法であって、

上記複数のルータ装置間に、上記経路情報を通知するための、上記構築されるＶＰＮに対応した通信路を設定するステップと、

上記通信路を介して該通信路に対応するＶＰＮに含まれるユーザ網の経路情報を通知するステップとを有することを特徴とする経路情報通知方法。

【請求項８】請求項７記載の経路情報通知方法であって、

前記通信路を設定するステップは、前記構築されるＶＰＮの識別情報を用いて前記通信路の設定を要求するステップを有することを特徴とする経路情報通知方法。

【請求項９】請求項８記載の経路情報通知方法であって、

前記識別情報は、前記構築されるＶＰＮに対応したＩＰアドレスであることを特徴とする経路情報通知方法。

【請求項１０】複数のユーザ網を相互に接続し、該複数のユーザ網間での情報の送受信のための仮想的な専用通信路を設定して、該複数のユーザ網を含むＶＰＮを構築するネットワークに、ユーザ網を接続するためのルータ装置であって、

ユーザ網と通信するための第一の通信手段と、

上記ネットワークに接続している他のルータ装置と通信するための第二の通信手段と、

上記第一の通信手段を介して通信するユーザ網を含むＶＰＮを構築するために、該ＶＰＮに含まれるユーザ網の経路情報を上記第二の通信手段を介して通信する他のルータ装置との間で送受信するための通信路を管理する通信路管理手段を有し、

上記通信路管理手段は、構築されるＶＰＮと対応付けて、上記通信路を管理し、

上記第二の通信手段は、ＶＰＮを構築するための経路情報を送信又は受信する場合に、上記通信路管理手段が該構築されるＶＰＮと対応付けて管理している通信路を用いることを特徴とするルータ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、仮想的なプライベートネットワークのサービスを行っているネットワークシステムにおいて、エッジルータ間で、ユーザ網の経路を交換するための技術に関する。

【０００２】

【従来の技術】ネットワーク技術の急速な進歩により、企業などで自社建物内の計算機を接続し、WWW（World Wide Web）やメールなどのアプリケーションを建物内で接続して使用したいという需要が増加している。建物内の計算機を相互に接続するＬＡＮ(Local Area Network)の普及により、それは広く実現された。次に、ユーザの需要は地域的に分散されて、ＬＡＮ整備されている各支店を接続することへと変化した。それを実現する技術として、網プロバイダが異なる位置の企業ユーザを接続するネットワークを提供する事によりユーザ側にて仮想的にプライベートな状態でそのネットワークを利用できる仮想プライベートネットワーク（ＶＰＮ）が注目されている。互いに遠隔地にあるユーザホスト間でＶＰＮを構築する方法として、通信事業者網のエッジ部分、すなわち顧客網との接点である周辺部分に置かれているエッジルータ間で、ＶＰＮ顧客の通信を論理的または物理的に多重化する方法が考えられる。これによりＶＰＮ顧客からはあたかも専用線でつながっているように見える。本方式では、インターネットプロトコルアドレスを顧客網も通信事業者網も使用できるので、本方式のＶＰＮを以下ＩＰ－ＶＰＮサービスと表記する。

【０００３】ＩＰ-ＶＰＮを実現する技術は、インターネット技術の標準化団体ＩＥＴＦ(Internet Engineering Task Force)が規定する標準文書であるＲＦＣ２５４７に開示されている。ＲＦＣ２５４７ではＩＰ－ＶＰＮサービスを構築するために、通信事業者のエッジルータに以下の処理をすることが述べられている。まずエッジルータはＶＰＮサイト毎に分離した経路テーブルを保持、管理する。そしてエッジルータ間で経路テーブルの経路をルーティングプロトコルであるＢＧＰを用いて交換する。エッジルータから他のエッジルータに経路を通知する際、通知先のエッジルータ内のどの経路テーブルに、通知する経路を書きこむかを特定するために、以下の拡張実装をエッジルータに施している。あるグループに属するＩＰアドレスの集合であり、ＩＰアドレスとサブネットマスク（ＩＰアドレスの始点から終点までの長さ）の組に相当する経路のプレフィックスに加えて、その経路をどの経路テーブルに書きこむかを特定する識別子をＢＧＰで通知する経路メッセージに付加し、経路受け取り先のエッジルータはその識別子を見て、自分で管理しているＶＰＮサイト毎の経路テーブルに書きこむ。言い換えれば、図１８にて具体的に示す様にＢＧＰピア（すなわち、ＢＧＰプロトコルを実装された２台のルータ間の経路交換通知手段）１９０－Ａをエッジルータ１５０間に１つ張り、複数のＶＰＮユーザ網１００－Ａ、１００－Ｂ、１１０－Ａ、１１０－Ｂで共用する為、経路通知メッセージにデータ通信路で用いるＶＰＮ識別子を付加する必要が生じる。図１８では、さらにエッジルータ１５０間にデータパケット送信用としてトンネル（データ通信路）１９５が１つ設けられている。これらＢＧＰピアとトンネルは相互に独立して機能する。

【０００４】

【発明が解決しようとする課題】ＩＰ－ＶＰＮサービスを行う際の従来技術には、以下の２つの問題がある。

【０００５】第一の問題は、ＢＧＰの経路通知メッセージに経路テーブルの識別子を付加するため、ＢＧＰプロトコルを拡張する必要がある、ということである。このため、既存のＢＧＰプロトコルに基づいて設計されたルータとの相互接続が不可能となる。第二の問題は、エッジルータが受信した経路情報各々に対して、取込み先指定(反映する経路テーブルの選択)などの経路フィルタ機能を実現する場合、既存のフィルタ機能を流用できないことである。ＶＰＮという概念をもたない既存のＢＧＰプロトコルでは、経路フィルタ機能には以下の３つが存在していた。１つめは、経路送受信に使用されたＢＧＰピア単位で、そのピア（通信路）を経由した経路を格納または廃棄するかを選択できるフィルタである。２つめは、ＩＰアドレスとサブネットマスクの組であるプレフィックス単位で、経路を格納または廃棄するかを選択できるフィルタである。３つめは、上記２つのフィルタを合わせた形で、経路送信用ＢＧＰピアとＩＰアドレスの組で、経路を格納または廃棄するかを選択できるフィルタである。

【０００６】しかし、これらの機能では、経路通知メッセージに付加されたＶＰＮ識別子を用いたフィルタリングが行えない為、既存のフィルタを用いてＶＰＮサイト毎に経路テーブルを分離することが出来ない。

【０００７】これらの問題は、ＶＰＮサービスを提供しようとする場合、仮想プライベート網内の全エッジルータのソフトウェア更新あるいは装置交換が必要となることを意味し、導入コストが著しく上昇することにつながる。

【０００８】

【課題を解決するための手段】本発明では、通信事業者の網内にエッジルータを設置し、それをＶＰＮ顧客網のルータと回線でつなげる。通信事業者のエッジルータは、ＶＰＮ顧客網のルータより、それが設置されているＶＰＮサイトの経路を受け取る。

【０００９】通信事業者のエッジルータは、ルーティングプロトコルを用いて、受け取った経路を通信事業者の他のエッジルータに通知する。経路を受け取った他のエッジルータは、以下に示す方法でその経路に対応するＶＰＮを認識し、認識したＶＰＮに対応する経路テーブルに経路を書きこむと共に、接続しているユーザ網のルータにその経路を通知する。

【００１０】以上により、ユーザ網の経路が交換される。

【００１１】通信事業者のエッジルータがＶＰＮ顧客の経路を受け取ったとき、そのＶＰＮを識別する方法を示す。本発明では、経路情報のパケットであるＵＰＤＡＴＥメッセージ（経路削除/追加及びＩＰアドレスに対するパス属性から成る）とも呼ばれる経路通知メッセージにＶＰＮ識別子を含めず、経路通知メッセージを送受信する為のＢＧＰのピアをエッジルータ間に張るよう要求する接続要求メッセージを用いてＶＰＮを識別する。

【００１２】接続要求メッセージによってＶＰＮを識別する方法は例えば以下の２つがある。

【００１３】第一の方法は、エッジルータが接続要求メッセージを受信する時に、接続要求メッセージに含まれる接続相手のＩＰアドレスによってＶＰＮを識別する。あらかじめエッジルータの管理者によって登録していた接続相手のＩＰアドレスとＶＰＮ識別子の対応表を参照することで、接続要求メッセージとＶＰＮ識別子との対応付けが可能となる。第二の方法は、エッジルータが接続要求メッセージを送信する時に、接続要求のメッセージにＶＰＮ識別子を付加することで、接続要求を受ける側のエッジルータは接続要求メッセージからＶＰＮを識別するものである。接続要求メッセージは、ＯＰＥＮメッセージとも呼ばれＢＧＰヘッダ（送り手アドレスであるＢＧＰ－ＩＤから成る）とＩＰヘッダ（送信元/送信先を示すＩＰアドレス）から構成される。この方法では、接続要求を受け取った側のエッジルータでは要求メッセージ中のＶＰＮ識別子を即座に自分の構成定義にあるＶＰＮ識別子と比較することができる。

【００１４】エッジルータは接続要求メッセージからＶＰＮを識別したら、そのＶＰＮに関する経路通知メッセージを送受信する為のＢＧＰピアを張る。

【００１５】従って、エッジルータはＢＧＰピア毎にそのＢＧＰピアを経由して送受信される経路通知メッセージがどのＶＰＮに対応するものかを識別することができる。

【００１６】これにより経路通知メッセージを拡張することなくＶＰＮ顧客の経路をエッジルータ間で交換することが出来る。又、経路フィルタについても、本方式ではＢＧＰピアがＶＰＮユーザ単位に用意されるので、既存のＢＧＰピア単位のフィルタをそのままＶＰＮユーザ単位のフィルタとして流用することができる。さらに本発明は、１つの物理ネットワークに接続される特定のユーザに対して、仮想的な専用通信路をユーザ毎に提供する複数のＶＰＮユーザに対するＶＰＮサービスであって、物理ネットワーク網に存在し、ユーザ網との接点部分に配置される複数個エッジルータ装置を有し、各エッジルータ装置はＶＰＮユーザに関連した経路テーブルを有し、複数個エッジルータ装置間には少なくとも複数のＶＰＮユーザに対して独立した経路情報通知手段が設けられていることを特徴とするＶＰＮサービスを提供する事である。さらに本発明は、１つの物理ネットワークに接続される特定のユーザに対して、仮想的な専用通信路をユーザ毎に提供するＶＰＮサービスに用いられるエッジルータ装置であって、そのエッジルータ装置は物理ネットワーク網に存在し、ユーザ網との接点部分に複数個配置され、各々のエッジルータ装置はＶＰＮユーザに関連した経路テーブルを有し、複数個のエッジルータ装置間にはＶＰＮユーザ毎に独立した経路情報通知手段が設けられ得ることを特徴とするエッジルータ装置を提供する事である。

【００１７】さらに本発明は、複数のユーザ網と、該複数のユーザ網を相互に接続するネットワークとを有するネットワークシステムにおいて、上記複数のユーザ網間で情報の送受信を行うための仮想的な専用通信路を上記ネットワークに設定して、該複数のユーザ網を含むＶＰＮを構築するための経路情報を、該複数のユーザ網の各々を該ネットワークに接続する複数のルータ装置間で通知するための方法であって、上記複数のルータ装置間に、上記経路情報を通知するための、上記構築されるＶＰＮに対応した通信路を設定するステップと、上記通信路を介して該通信路に対応するＶＰＮに含まれるユーザ網の経路情報を通知するステップとを有することを特徴とする経路情報通知方法を提供する事である。

【００１８】上記経路情報通知方法において、前記通信路を設定するステップは、前記構築されるＶＰＮの識別情報を用いて前記通信路の設定を要求するステップを有することを特徴とする。

【００１９】上記経路情報通知方法において、前記識別情報は、前記構築されるＶＰＮに対応したＩＰアドレスであることを特徴とする。

【００２０】さらに本発明は、複数のユーザ網を相互に接続し、該複数のユーザ網間での情報の送受信のための仮想的な専用通信路を設定して、該複数のユーザ網を含むＶＰＮを構築するネットワークに、ユーザ網を接続するためのルータ装置であって、ユーザ網と通信するための第一の通信手段と、上記ネットワークに接続している他のルータ装置と通信するための第二の通信手段と、上記第一の通信手段を介して通信するユーザ網を含むＶＰＮを構築するために、該ＶＰＮに含まれるユーザ網の経路情報を上記第二の通信手段を介して通信する他のルータ装置との間で送受信するための通信路を管理する通信路管理手段を有し、上記通信路管理手段は、構築されるＶＰＮと対応付けて、上記通信路を管理し、上記第二の通信手段は、ＶＰＮを構築するための経路情報を送信又は受信する場合に、上記通信路管理手段が該構築されるＶＰＮと対応付けて管理している通信路を用いることを特徴とするルータ装置を提供する事である。

【００２１】

【発明の実施の形態】以下，図面を用いて本発明につい

て説明する。

【００２２】図１はＶＰＮのシステム構成を示している。本システムは、通信事業者網１２０とユーザ網１００－Ａ、１００－Ｂ、１１０－Ａ、１１０－Ｂで構成される。１００－Ａと１１０－Ａはあるユーザ網、１００－Ｂ、１１０－Ｂは別のユーザ網とする。１００－Ａからは１１０－Ａへは通信事業者網上で正常に通信を行うことが出来る。１００－Ａから１００－Ｂや１１０－Ｂへの通信はユーザが異なるため、通信を遮蔽する。ユーザ網が異なるとアドレス空間も異なる。例えばあるユーザ網で使用しているＩＰアドレスは、他のユーザ網で使用することも可能である。

【００２３】エッジルータ１５０内の経路テーブル１６０または１７０はＶＰＮ毎に管理される。エッジルータ１５０－Ａ内の経路テーブル１６０－Ａは、経路テーブルに対応するユーザ網１００－Ａ内の経路をユーザ網のルータ１３０－Ａから受け取り、書き込む。そして同じＶＰＮに所属する別のエッジルータ１５０－Ｂ内の経路テーブル１７０－Ａから通知された経路も書き込む。エッジルータ１５０間のＶＰＮ経路の交換の前準備として、ＶＰＮ毎に独立した経路交換通知手段を用意する必要がある。経路交換通知手段の例としてＢＧＰプロトコルのピアがある。実際はＩＰネットワーク上で通信を保証されたＴＣＰ（Transfer Control Protocol）接続のことで、そのＴＣＰ接続を用いて経路が交換される。以降の説明では、経路交換通知手段をＢＧＰピアという用語を用いて説明する。

【００２４】ＶＰＮ毎にＢＧＰピア１９０－Ａ、１９０－Ｂを用意する。ＢＧＰピア上を流れる経路通知パケットにはＶＰＮを識別する情報は含めない。経路情報を受信したエッジルータは、ＢＧＰピアとＶＰＮ識別子の対応表であるＢＧＰピア管理テーブル３４６（図５にて詳述する）を参照して、通知された経路のＶＰＮを特定する。

【００２５】ＶＰＮサイト間の通信はエッジルータ１５０間で通信路を設定し、その通信路にＶＰＮのデータパケットを流すことで行われる。コアルータ１８０はＶＰＮの経路テーブルを保持せず、設定された通信路を用いてＶＰＮのデータパケットを中継する。

【００２６】図２はエッジルータ１５０のハードウェア構成を示している。

【００２７】ＣＰＵ（Central Processing Unit）２００はメモリ２１０に格納されているプログラムを実行するためのプロセッサである。メモリ２１０の中には装置全体を制御するためのオペレーティングシステム２１３，およびルータ装置としての動作を行うための制御プログラム２１５が格納されている。

【００２８】ユーザ網側ネットワークコントローラ２２０はエッジルータ１５０がユーザ網のルータとの間で行う送受信を制御する。通信事業者網側ネットワークコントローラ２２５は、エッジルータ１５０が相手のエッジルータ１５０との間で行う送受信を制御する。キーボードコントローラ２３０はキーボード２３５からのキー入力を制御する。シリアルコントローラ２４０はシリアルポートに接続されたマウス２４５などの入出力機器を制御する。ディスプレイコントローラ２５０はディスプレイモニタ２５５への画面表示を制御する。ディスクコントローラ２６０はディスク装置２６５への入出力を制御する。

【００２９】なお，本実施例においては，ネットワーク管理者によるエッジルータ１５０の操作は装置に直接接続されたキーボード２３５，マウス２４５，ディスプレイモニタ２５５から行うことを前提としているが，エッジルータ１５０とネットワークを介してつながった遠隔地にある入出力装置を用いて操作を行うこともちろん可能である。

【００３０】図３はエッジルータ１５０のソフトウェア構成を示している。

【００３１】入出力制御部３１０はキーボードからの入力やディスプレイへの出力を制御する。

【００３２】ユーザ網側ネットワークインタフェース部３８０は、ユーザ網側のルータから受信したパケットをユーザ網側通信部３６０に渡したり、ユーザ網側通信部３６０の要求により、パケットをネットワークに送信するなど、ユーザ網側のルータとの間の送受信に関する処理を行う。

【００３３】通信事業者網側ネットワークインタフェース部３９０は、他の通信事業者網側のエッジルータ１５０から受信したパケットを通信事業者網側通信部３７０に渡したり、通信事業者網側通信部３７０の要求により、パケットをネットワークに送信するなど、通信事業者網側のエッジルータ１５０との間の送受信に関する処理を行う。

【００３４】ユーザ網側通信部３６０は、ユーザ網側ネットワークインタフェース部３８０から受信したパケットを、その結果に応じてルーティングプロトコルパケット解析部３４０、データ中継部３５０の内の適切な処理モジュールの方へ渡したり、これらの処理モジュールから渡されたパケットに適切なヘッダを付加してユーザ網側ネットワークインタフェース部３８０に渡すなど、内部プロトコルに応じたパケットヘッダの解釈と各モジュールへのパケット振分処理を行う。ここで該ユーザ網側通信部３６０は、ユーザ網と通信するための第一の通信手段とする。

【００３５】通信事業者網側通信部３７０は、通信事業者網側ネットワークインタフェース部３９０から受信したパケットを、その結果に応じてルーティングプロトコルパケット解析部３４０、データ中継部３５０の内の適切な処理モジュールの方へ渡したり、これらの処理モジュールから渡されたパケットに適切なヘッダを付加して

通信事業者網側ネットワークインタフェース部３９０に渡すなど、内部プロトコルに応じたパケットヘッダの解釈と各モジュールへのパケット振分処理を行う。ここで該通信事業者網側通信部３７０は、ネットワークに接続している他のエッジルータ装置と通信するための第二の通信手段とする。

【００３６】データ中継部３５０は、ユーザ網側通信部３６０と通信事業者網側通信部３７０、ルーティングプロトコルパケット解析部３４０のデータを中継し、パケットのヘッダを参照し、どの機能ブロックへ転送するかを決定する。さらにデータ転送の場合は経路テーブル１６０又は１７０を参照し、送出するインターフェースを決定する。

【００３７】ルーティングプロトコルパケット解析部３４０は、ルーティングプロトコルのパケットを解析後、経路を追加または削除するために、経路情報を経路フィルタ管理部３３０に渡す。またＢＧＰの接続要求パケットが正常なら、それを登録するためＢＧＰピア管理部３４４に接続を依頼する。

【００３８】ＢＧＰピア管理部３４４は、ＢＧＰの接続が成功した場合にその接続を保持する。ここで該ＢＧＰピア管理部３４４は、上記第一の通信手段を介して通信するユーザ網を含むＶＰＮを構築するために、該ＶＰＮに含まれるユーザ網の経路情報を上記第二の通信手段を介して通信する他のエッジルータ装置との間で送受信するための通信路を管理する通信路管理手段とする。接続情報はＢＧＰピア管理テーブル３４６へ書き込まれる。

【００３９】経路フィルタ管理部３３０は、ルーティングプロトコルパケット解析部３４０により経路の追加または削除の要求があったとき、経路の追加を制限する経路フィルタ表３３５を参照して、それを許可するかどうかを決める。

【００４０】経路テーブル管理部３２０は、経路フィルタで許可された経路を、ＶＰＮ毎に管理された経路テーブル１６０または１７０に書き込み、それぞれの経路テーブルはＶＰＮに対応しているので、どのＶＰＮに経路を書き込むかをＢＧＰピア管理テーブル３４６を参照して特定する。また経路テーブル管理部３２０は、データパケット転送のために経路テーブル１６０または１７０の検索を行う。

【００４１】図４はエッジルータ１５０が使用する経路テーブル１６０または１７０の形式を示している。本経路テーブルはＶＰＮ毎に分離して、ルータ内で保持される。

【００４２】経路テーブル１６０または１７０には，各ＶＰＮの経路情報がテーブル形式で格納されている。各経路情報には経路のＩＰアドレス４１０、ネットワークＩＤとホストＩＤから構成されるＩＰアドレスの内、ネットワークＩＤの長さを特定するために用いられるサブネットマスク４２０，ＮｅｘｔＨｏｐ４３０、インターフェース識別子４４０、経路送信元ルータのＩＰアドレス４５０、経路の属性４６０が含まれる。

【００４３】経路のＩＰアドレス４１０、サブネットマスク４２０及びＮｅｘｔＨｏｐ４３０は、他ルータより通知される。ＮｅｘｔＨｏｐ４３０は経路を通知した送信元ルータに到達するために、エッジルータ１５０がデータパケットを転送する次のルータのアドレスを示している。インターフェース識別子４４０は、ＮｅｘｔＨｏｐ４３０に繋がっているエッジルータ１５０側のインターフェースを特定するための識別子である。

【００４４】経路送信元ルータのＩＰアドレス４５０は、経路送信元のＢＧＰピアを識別する。経路送信元ルータのＩＰアドレスは、経路フィルタに用いられる。例えばあるＢＧＰピアから来た経路を全て経路テーブル１６０または１７０に書き込まないという管理者の設定に対応する際、経路がどのＢＧＰピアから通知されたかという経路送信元ルータのＩＰアドレス４５０が参照される。

【００４５】経路の属性４６０は、ＢＧＰプロトコルで規定されている。例えば同一経路が複数のＢＧＰピアから通知された場合、どの経路を採用するかという経路のコストを規定する。

【００４６】図５はエッジルータが使用するＢＧＰピア管理テーブル３４６の形式を示している。

【００４７】図５のＢＧＰピア管理テーブル３４６にはＢＧＰピア識別子５１０、接続相手のＩＰアドレス５２０、ＶＰＮ－ＩＤ５３０が含まれる。ＢＧＰピア識別子５１０は、この装置内で保持するＢＧＰピアを識別する番号である。接続相手のＩＰアドレス５２０とＶＰＮ－ＩＤ５３０は、ＢＧＰの接続要求を受けたとき、その接続のＶＰＮを特定するため使用される。

【００４８】接続要求とは、エッジルータが他のエッジルータとの間で経路交換を行うためにＢＧＰピアを張るよう該他のエッジルータに要求する処理であり、エッジルータは経路交換の許可をとるために該他のエッジルータに対して、自エッジルータの情報を通知する。接続要求受信側ルータは、送信側に対して接続を認める、または認めないのどちらかを選択し、その返事を接続要求側ルータに返す。接続要求を認められたルータは、ＢＧＰピアを張り、ＢＧＰプロトコルにしたがってＢＧＰピアを用いて経路を通知することができる。ＢＧＰピアが張られた２台のＢＧＰルータ間では、経路情報が自動的に交換される。

【００４９】図６はエッジルータ１５０のＶＰＮ経路登録及び登録後のエッジルータ１５０間でのＶＰＮ経路の交換を示すシーケンスである。エッジルータＡの管理者はまずユーザ網のルータと経路交換用のＢＧＰピアを接続する設定を行う（シーケンス６１０－Ａ）。その設定はエッジルータＢの場合も同様で（シーケンス６１０－Ｂ）、エッジルータＡとエッジルータＢの設定順序は問

わない。

【００５０】管理者からＢＧＰピアの設定を受けたエッジルータＡは、ユーザ網のルータＡに対して経路交換用のピアの接続要求を出す（シーケンス６２０－Ａ）。接続要求を受けたユーザ網のルータＡは接続要求を受け入れる場合はＡＣＫを返し、拒否する場合にはエラー通知であるＮＯＴＩＦＹを返す（シーケンス６３０－Ａ）。エッジルータＡは、通信事業者網の他のエッジルータであるＢに対して経路交換用のＢＧＰピアを接続するために接続要求メッセージを送信する（シーケンス６４０）。接続要求メッセージを受けたエッジルータＢは要求を受け入れる場合はＡＣＫを返し、そうでない場合はＮＯＴＩＦＹを返す（シーケンス６５０）。以上によりユーザ網側と通信事業者網側両方にＢＧＰピアを接続した後、経路がユーザ網のルータＡよりエッジルータＡに通知される。通知を受けたエッジルータＡは、その経路をルータ内に保持するＶＰＮユーザ毎の経路テーブルに書き込み、その経路を通信事業者網に存在する他エッジルータであるＢに通知する（シーケンス６６０－Ａ）。エッジルータＢも同様にしてＶＰＮ経路をエッジルータＡに通知する（シーケンス６６０－Ｂ）。

【００５１】図７はエッジルータＡのＶＰＮ削除を示すシーケンスである。エッジルータＡのみで、あるユーザ網が削除された場合を示す。

【００５２】エッジルータＡの管理者は、エッジルータＡに対してユーザ網Ａにあらかじめ貼ってあるＢＧＰピアの削除を設定する（シーケンス７１０）。ＢＧＰピア削除の命令を受けたエッジルータＡは、ユーザ網のルータＡに対してＢＧＰピアの削除要求を出す（シーケンス７２０）。削除要求を受けたユーザ網のルータＡはその削除要求が正常に動作できるかを確認した後、削除を許容するかエラーを返す（シーケンス７３０）。ユーザ網のルータＡ、エッジルータＡともにエッジルータＢから通知された経路をＢＧＰピア毎に保持しているので、エッジルータＡとの間に貼ってあるＢＧＰピアの削除に伴い、そのＢＧＰピアから通知された全経路をユーザ網のルータＡ内の経路テーブルから削除する。

【００５３】ユーザ網のルータＡからの削除応答を受けたエッジルータＡは、エッジルータＢに対してＢＧＰピアの削除要求を出す（シーケンス７４０）。ピアの削除要求を受けたエッジルータＢはルータ内のＢＧＰピア管理テーブルから削除要求のあったピアを削除し、ＡＣＫを返す（シーケンス７５０）。ＢＧＰピアの削除前にエッジルータＡからエッジルータＢに通知された経路は、ピアの削除時にＶＰＮ毎の経路テーブルから削除される。

【００５４】図８はエッジルータＡ及びエッジルータＢでのＶＰＮ削除を示すシーケンスである。

【００５５】エッジルータＡの管理者は、エッジルータＡに対してユーザ網Ａにあらかじめ貼ってあるＢＧＰピアの削除を設定する（シーケンス８１０－Ａ）。エッジルータＢの管理者も同様にエッジルータＢに対してユーザ網Ｂにあらかじめ貼ってあるＢＧＰピアの削除を設定する（シーケンス８１０－Ｂ）。

【００５６】ＢＧＰピア削除の命令を受けたエッジルータＡは、ユーザ網のルータＡに対してＢＧＰピアの削除要求を出す（シーケンス８２０－Ａ）。通信事業者網ルータ装置Ｂも同様にＢＧＰピア削除の命令を受けたエッジルータＢは、ユーザ網のルータＢに対してＢＧＰピアの削除要求を出す（シーケンス８２０－Ｂ）。削除要求を受けたユーザ網のルータＡはその削除要求が正常に動作できるかを確認した後、削除を許容するかエラーを返す（シーケンス８３０－Ａ）。ユーザ網ルータＢ側でも同様に削除要求を受けたユーザ網のルータＢはその削除要求が正常に動作できるかを確認した後、削除を許容するかエラーを返す（シーケンス８３０－Ｂ）。

【００５７】ユーザ網ルータＡ及びＢ側のＢＧＰピア削除が完了した後、エッジルータＡ及びＢは、エッジルータ間のＢＧＰピア削除を行う（シーケンス８４０、８５０）。

【００５８】図９はユーザ網間のデータ通信のシーケンスである。データ通信の前準備としてエッジルータＡ，Ｂはユーザ網の経路を交換し終えたものとする。ユーザ網のルータＡからユーザ網のルータＢにデータパケットを通信するシーケンスを示す。

【００５９】ユーザ網のルータＡは、エッジルータＡにデータパケットを送信する（シーケンス９１０）。データパケットを受信したエッジルータＡは、データパケットのＶＰＮに対応する経路テーブルを参照し、エッジルータＢにデータパケットを転送する（シーケンス９２０）。エッジルータＢはデータパケットを受け取り、データパケットのＶＰＮに対応する経路テーブルを参照して、データパケットをユーザ網のルータＢに転送する（シーケンス９３０）。

【００６０】図１０はエッジルータ１５０の、ユーザ網のルータとのＢＧＰピア接続要求フローである。ネットワーク管理者から接続要求を入力（ステップ１００５）されたエッジルータ１５０はＢＧＰプロトコルの接続要求メッセージを、指定されたＩＰアドレスをもつユーザ網のルータに送信する（ステップ１０１０）。その後エッジルータ１５０はユーザ網のルータから接続のＡＣＫを待つ。もしユーザ網のルータがエッジルータ１５０の接続要求をエラーなどの理由で拒否するときは、ユーザ網のルータはエッジルータ１５０にエラーメッセージであるＮＯＴＩＦＹを返す（ステップ１０２０）。もしＡＣＫではなくＮＯＴＩＦＹを受け取ったら、ディスプレイモニタへエラーを出力する（ステップ１０２５）。もし接続相手から正常にＢＧＰピアを接続したことを示すＡＣＫを受信したら（ステップ１０３０）、接続に成功したＢＧＰピア情報をＢＧＰピア管理テーブル３４６に

追加する（ステップ１０４０）

図１１はエッジルータ１５０の、ユーザ網のルータからのＢＧＰピア接続要求の受信フローである。

【００６１】接続要求メッセージを受信する前に、エッジルータ１５０は接続を許容する相手ルータのＩＰアドレスを入力する（ステップ１１０５）。ＩＰアドレスを１つずつ羅列する設定や接続要求側の全てのＩＰアドレスを許容する設定を行う。その後接続相手ルータより接続要求メッセージを受信する（ステップ１１１０）。接続要求メッセージを受けた受信側エッジルータ１５０は、接続要求メッセージをチェックする。もし接続要求メッセージパケットに異常を発見したり（ステップ１１２０）、上記の接続を許容する相手のＩＰアドレスに設定していない接続相手からの要求メッセージが到着した場合（ステップ１１３０）、接続を確立せず、接続要求元ルータにエラーメッセージであるＮＯＴＩＦＹを送信し（ステップ１１２５）、ディスプレイモニタへエラーを出力する（ステップ１１３５）。

【００６２】接続を許容する場合、接続相手にＡＣＫを返信し（ステップ１１４０）、接続要求受信側エッジルータ１５０は、ルータ内のＢＧＰピア管理テーブル３４６に新たなＢＧＰピアを登録する。図１２はエッジルータ１５０間でＢＧＰピア接続をする際の、エッジルータ１５０の接続要求処理のフローを示す。

【００６３】ＢＧＰピアのＶＰＮを識別する方法として接続要求メッセージに明示的にＶＰＮ－ＩＤを付加する方式を前提として示す。ネットワーク管理者はＢＧＰピア接続先のＩＰアドレスとＶＰＮ－ＩＤを組でエッジルータ１５０に設定する（ステップ１２０５）。管理者からの設定を受けたエッジルータ１５０はＶＰＮ－ＩＤ付きの接続要求メッセージを接続相手のエッジルータ１５０に送信する（ステップ１２１０）。その後接続ＡＣＫを待つ。もし接続相手のエッジルータ１５０が接続を拒否した場合、エラーとその原因を示すＮＯＴＩＦＹが接続要求側のエッジルータ１５０に返送される（ステップ１２２０）。ＮＯＴＩＦＹを受信したエッジルータ１５０はそれを管理者に通知するため、ディスプレイモニタへエラーを出力する（ステップ１２２５）。正常にＢＧＰピアの接続が接続相手のエッジルータ１５０から許可された場合、接続要求を送信したエッジルータはＡＣＫを受信する（ステップ１２３０）。ＡＣＫを受信したエッジルータ１５０は新たに接続するＢＧＰピアを管理テーブル３４６に追加する（ステップ１２４０）。

【００６４】図１３はエッジルータ１５０間でＢＧＰピア接続をする際の、エッジルータ１５０の接続受信側処理のフローを示す。ＢＧＰピアのＶＰＮを識別する方法として接続要求メッセージに明示的にＶＰＮ－ＩＤを付加する方式を前提として示す。ネットワーク管理者は他エッジルータ１５０から接続要求メッセージを受信する前に、接続を許容する相手のＩＰアドレスを登録する（ステップ１３０５）。その後接続要求メッセージを受信し（ステップ１３１０）、受信した接続要求メッセージをチェックする。もし接続要求メッセージパケットに異常が発見されたり（ステップ１３２０）、接続を許容する相手のＩＰアドレスに一致しない（ステップ１３３０）、接続要求メッセージに含まれるＶＰＮ－ＩＤの値が異常である（ステップ１３４０）、等の場合は接続を拒否する。エラーを接続要求元のエッジルータ１５０に通知するため、ＮＯＴＩＦＹを送信し（ステップ１３２５）、ルータ管理者に通知するため、ディスプレイモニタへエラーを出力する（ステップ１３３５）。接続要求を受け入れる場合、接続要求側にＡＣＫを返信する（ステップ１３５０）。新たな接続を登録するため、ＢＧＰピア管理テーブル３４６に追加する（ステップ１３６０）。

【００６５】図１４はエッジルータ１５０間でＢＧＰピア接続をする際の、エッジルータ１５０の接続要求処理のフローを示す。ＢＧＰピアのＶＰＮを識別する方法として接続要求を受信したエッジルータ１５０が接続相手のＩＰアドレスとＶＰＮ－ＩＤを対応させる方式を前提として示す。

【００６６】ネットワーク管理者はＢＧＰピア接続先のＩＰアドレスとＶＰＮ－ＩＤを組でエッジルータ１５０に設定する（ステップ１４０５）。管理者からの設定を受けたエッジルータ１５０は接続要求メッセージを接続相手のエッジルータ１５０に送信する（ステップ１４１０）。その後接続ＡＣＫを待つ。もし接続相手のエッジルータ１５０が接続を拒否した場合、エラーとその原因を示すＮＯＴＩＦＹが接続要求側のエッジルータ１５０に返送される（ステップ１４２０）。ＮＯＴＩＦＹを受信したエッジルータ１５０はそれを管理者に通知するため、ディスプレイモニタへエラーを出力する（ステップ１４２５）。正常にＢＧＰピアの接続が接続相手のエッジルータ１５０から許可された場合、接続要求を送信したエッジルータ１５０はＡＣＫを受信する（ステップ１４３０）。ＡＣＫを受信したエッジルータ１５０は新たに接続するＢＧＰピアを管理テーブル３４６に追加する（ステップ１４４０）。

【００６７】図１５はエッジルータ１５０間でＢＧＰピア接続をする際の、エッジルータ１５０の接続受信側処理のフローを示す。ＢＧＰピアのＶＰＮを識別する方法として接続要求を受信したエッジルータ１５０が接続相手のＩＰアドレスとＶＰＮ－ＩＤを対応させる方式を前提として示す。ネットワーク管理者は他エッジルータ１５０から接続要求メッセージを受信する前に、接続を許容する相手のＩＰアドレスと対応するＶＰＮ－ＩＤを登録する（ステップ１５０５）。その後接続要求メッセージを受信し（ステップ１５１０）、受信した接続要求メッセージをチェックする。もし接続要求メッセージパケットに異常が発見されたり（ステップ１５２０）、接続

を許容する相手のＩＰアドレスに一致しない（ステップ１５３０）場合は接続を拒否する。エラーを接続要求元のエッジルータに通知するため、ＮＯＴＩＦＹを送信し（ステップ１５２５）、ネットワーク管理者に通知するため、ディスプレイモニタへエラーを出力する（ステップ１５３５）。接続要求を受け入れる場合、接続相手のＩＰアドレスよりＶＰＮ－ＩＤを特定する（ステップ１５４０）。そして接続要求側にＡＣＫを返信する（ステップ１５５０）。新たな接続を登録するため、ＢＧＰピア管理テーブル３４６に追加する（ステップ１５６０）。

【００６８】図１６はエッジルータ１５０におけるＢＧＰピアの削除処理において、削除要求側のフローを示す。まずネットワーク管理者は、削除するＢＧＰピアのＩＰアドレスを入力する（ステップ１６０５）。次に削除要求メッセージをＢＧＰピア相手のエッジルータ１５０に送信する（ステップ１６１０）。その後接続削除相手のエッジルータ１５０からのＡＣＫを待つ。

【００６９】もし相手のエッジルータで削除が失敗したら、エラー通知であるＮＯＴＩＦＹメッセージが返信される（ステップ１６２０）。その場合、ネットワーク管理者にエラーを通知するため、ディスプレイモニタへエラーを出力する（ステップ１６２５）。もし相手のエッジルータ１５０が正常にＢＧＰピアを削除できたら、それを通知するＡＣＫが返信される（ステップ１６３０）。ＡＣＫを受信後、エッジルータ１５０はＢＧＰピア管理テーブル３４６から削除したピアのエントリを削除する（ステップ１６４０）。

【００７０】図１７はエッジルータ１５０におけるＢＧＰピアの削除処理において、削除要求受信側のフローを示す。エッジルータ１５０は、削除要求メッセージを受信する（ステップ１７１０）。もし接続要求メッセージに異常が存在したり（ステップ１７２０）、ＢＧＰピア管理テーブル３４６に削除メッセージで指定されたＢＧＰピアが存在しない場合、エラーメッセージであるＮＯＴＩＦＹを送信し、ディスプレイにエラー出力する。正常に削除が行われた場合、削除要求を送信した相手側エッジルータにＡＣＫを返信し（ステップ１７４０）、ＢＧＰピア管理テーブル３４６から該当するＢＧＰピアを削除する（ステップ１７５０）。以上でＶＰＮサービスを提供する物理網の管理者を通信事業者として例を挙げたが、企業ネットワークにも流用できることは明白である。

【００７１】

【発明の効果】以上で述べてきた方法を用いることにより、通信事業者が既存ルータを用いて、ＶＰＮサービスを容易に構築することが可能となる。

【００７２】従って、通信事業者がＶＰＮサービスを提供しようとする場合の導入コストが安価になるとともに、既存の設定知識が流用できるので、運用管理コストも安価になり、ユーザに安価なＶＰＮサービスを提供できる。

【図面の簡単な説明】

【図１】本発明のＶＰＮサービスにおけるネットワークシステムの構成図である。

【図２】本発明のエッジルータのハードウェア構成図である。

【図３】本発明のエッジルータのソフトウェア構成図である。

【図４】エッジルータが使用する経路テーブルを示す図である。

【図５】エッジルータが使用するＢＧＰピア管理テーブルを示す図である。

【図６】エッジルータ間のＶＰＮ登録の際のシーケンス図を示す図である。

【図７】片方のエッジルータでのＶＰＮ削除の際のシーケンス図である。

【図８】両方のエッジルータでのＶＰＮ削除の際のシーケンス図である。

【図９】ユーザ網のルータ間でのＶＰＮ通信のシーケンス図である。

【図１０】ユーザ網側へのＢＧＰピア接続要求のフローを示す図である。

【図１１】ユーザ網側へのＢＧＰピア接続受信のフローを示す図である。

【図１２】ＶＰＮ識別子を要求メッセージに含ませる方式の通信事業者側へのＢＧＰピア接続要求のフローを示す図である。

【図１３】ＶＰＮ識別子を要求メッセージに含ませる方式の通信事業者側へのＢＧＰピア接続受信のフローを示す図である。

【図１４】ＶＰＮの識別を、接続相手のアドレスで行う方式の通信事業者側へのＢＧＰピア接続要求のフローを示す図である。

【図１５】ＶＰＮの識別を、接続相手のアドレスで行う方式の通信事業者側へのＢＧＰピア接続受信のフローを示す図である。

【図１６】通信事業者側へのＢＧＰピア削除要求のフローを示す図である。

【図１７】通信事業者側へのＢＧＰピア削除受信のフローを示す図である。

【図１８】従来のＶＰＮサービスにおけるネットワークシステムの構成図である。

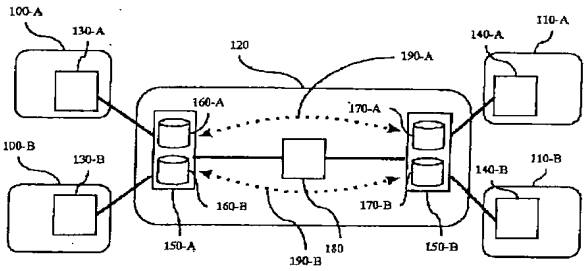
【符号の説明】

１００－Ａ、１００－Ｂ、１１０－Ａ、１１０－Ｂ…ユーザ網のネットワーク、１２０…通信事業者網のネットワーク、１３０－Ａ、１３０－Ｂ、１４０－Ａ、１４０－Ｂ…ユーザ網のルータ、１５０－Ａ、１５０－Ｂ…エッジルータ、１６０－Ａ、１６０－Ｂ、１７０－Ａ、１７０－Ｂ…経路テーブル、１８０…コアルータ、１９０

－Ａ、１９０－Ｂ…ＢＧＰピア、１９５…トンネル、２００…ＣＰＵ、２１０…メモリ、２１３…オペレーティングシステム、２１５…制御ソフト、２２０…ユーザ網側ネットワークコントローラ、２２５…通信事業者網側ネットワークコントローラ、２３０…キーボードコントローラ、２３５…キーボード、２４０…シリアルコントローラ、２４５…マウス、２５０…ディスプレイコントローラ、２５５…ディスプレイ、２６０…ディスクコントローラ、２６５…ディスク装置、３１０…入出力制御部、３２０…経路テーブル管理部、３３０…経路フィルタ管理部、３３５…経路フィルタ表、３４０…ルーティングプロトコルパケット解析部、３４４…ＢＧＰピア管理部、３４６…ＢＧＰピア管理テーブル、３５０…データ中継部、３６０…ユーザ網側通信部、３７０…通信事業者網側通信部、３８０…ユーザ網側ネットワークインターフェース部、３９０…通信事業者網ネットワークインターフェース部、４１０…経路のＩＰアドレス、４２０…経路のサブネットマスク、４３０…経路のＮｅｘｔＨｏｐ、４４０…Ｉ／Ｆ識別子、４５０…経路送信元ルータのＩＰアドレス、４６０…経路の属性、５１０…ＢＧＰピア識別子、５２０…接続相手のＩＰアドレス、５３０…ＶＰＮ－ＩＤ。

【図１】

図1



【図４】

図4

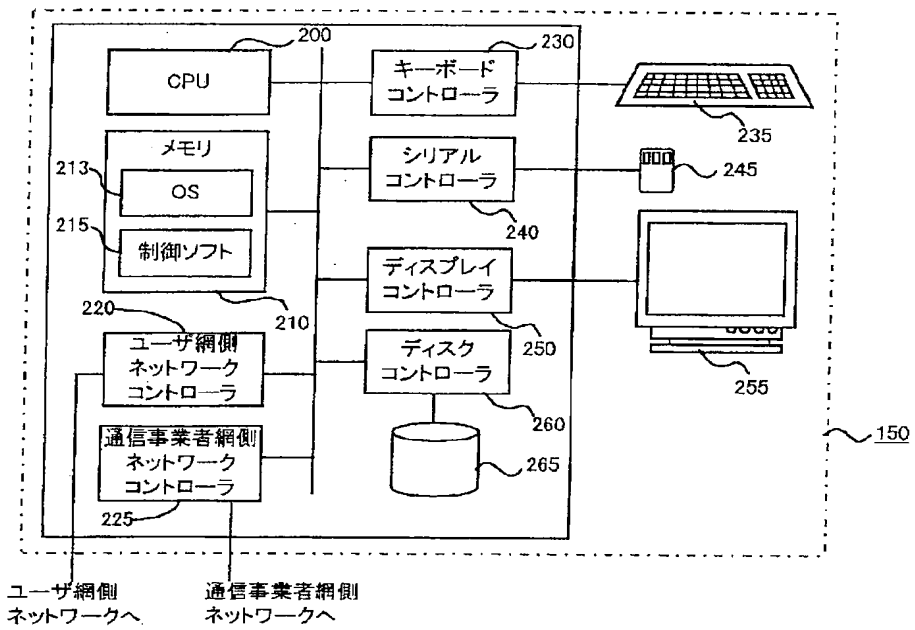
160または170

IPアドレス	サブネットマスク	NextHop	I/F識別子	経路送信元ルータのIPアドレス	経路の属性

410　420　430　440　450　460

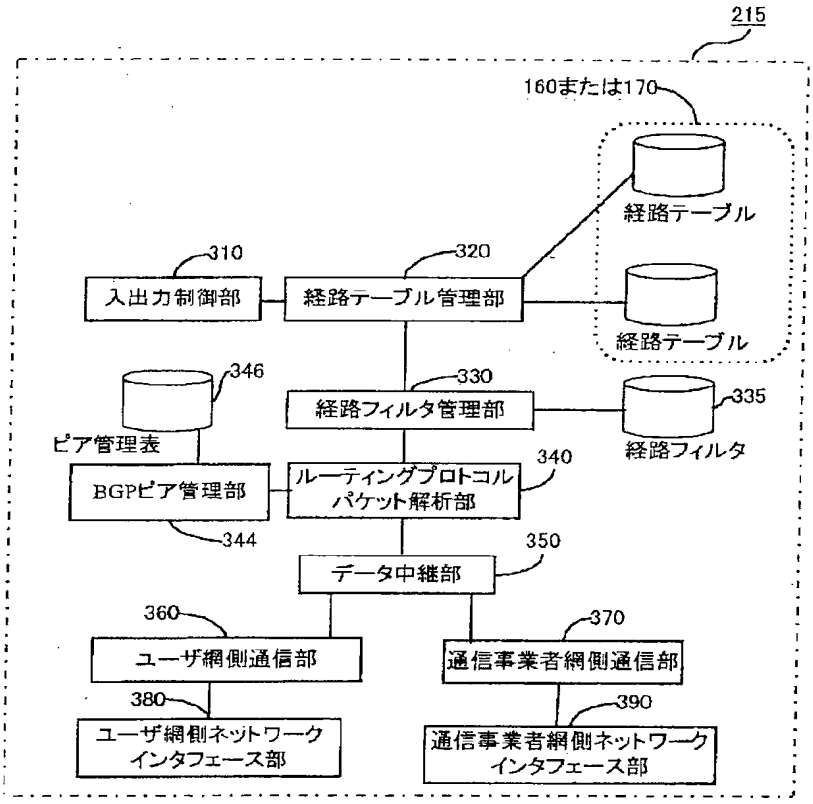
【図２】

図2



【図３】

図3



【図５】

図5

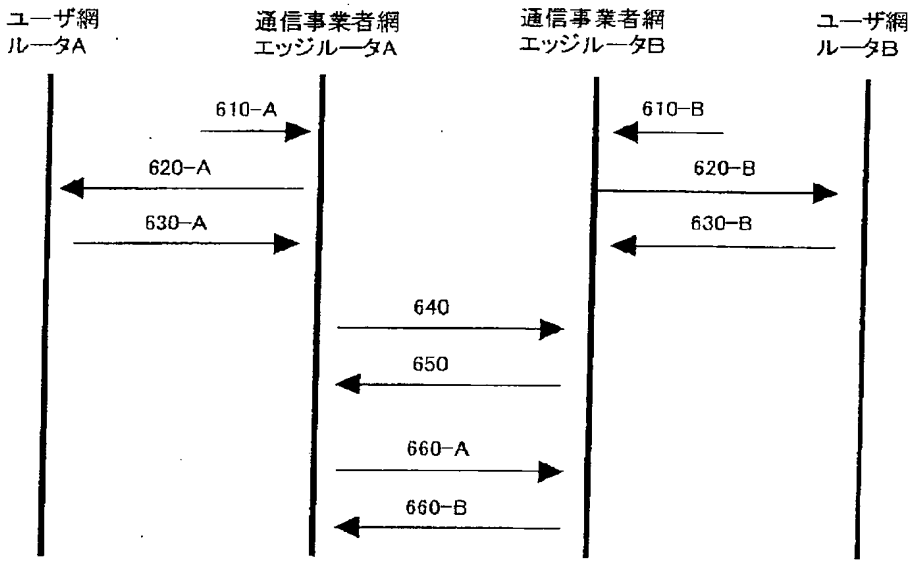
346

BGPピア識別子	接続相手のIPアドレス	VPN-ID

510 520 530

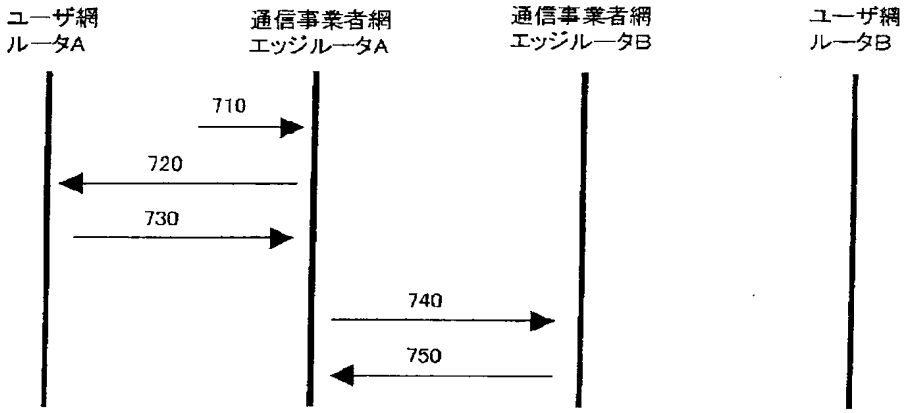
【図６】

図6


ユーザ網
ルータA
通信事業者網
エッジルータA
通信事業者網
エッジルータB
ユーザ網
ルータB
610-A
610-B
620-A
620-B
630-A
630-B
640
650
660-A
660-B

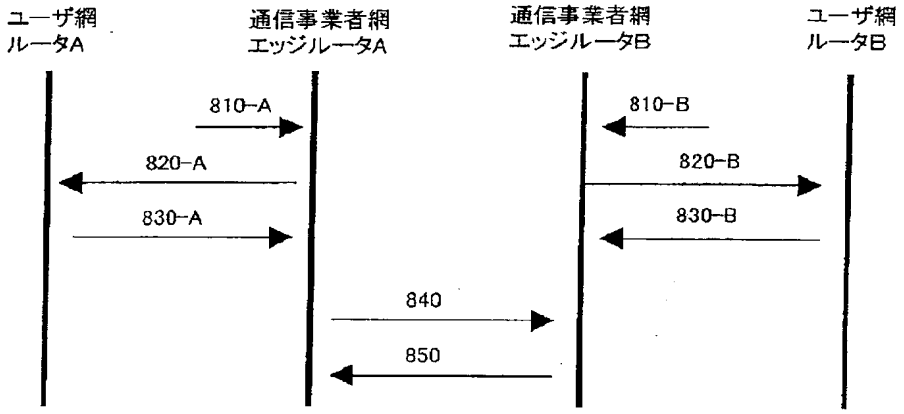
【図７】

図7


ユーザ網
ルータA
通信事業者網
エッジルータA
通信事業者網
エッジルータB
ユーザ網
ルータB
710
720
730
740
750

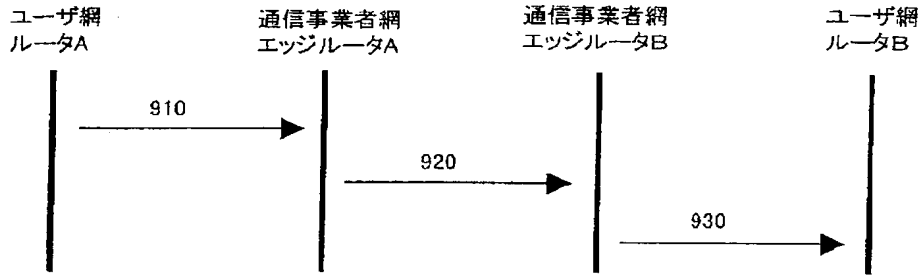
【図８】

図8



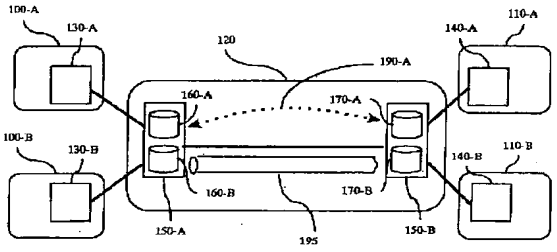
【図９】

図9



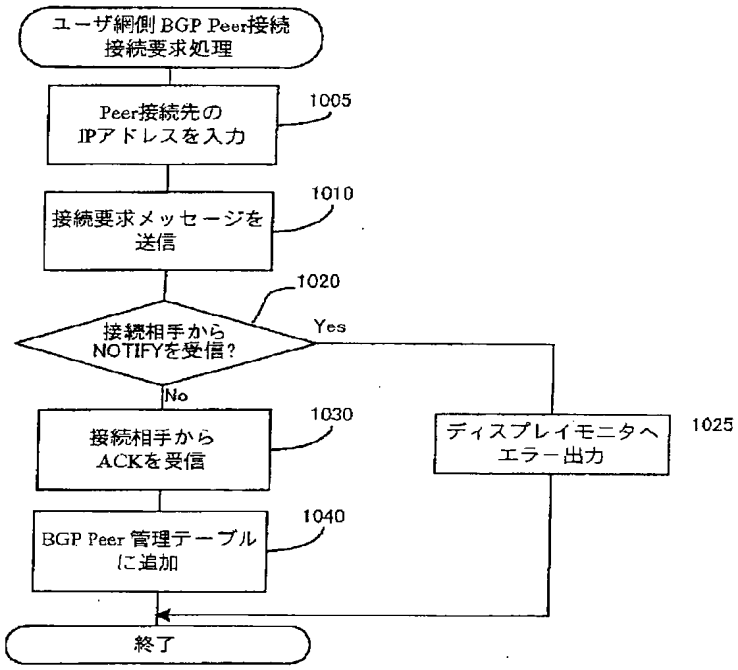
【図１８】

図18



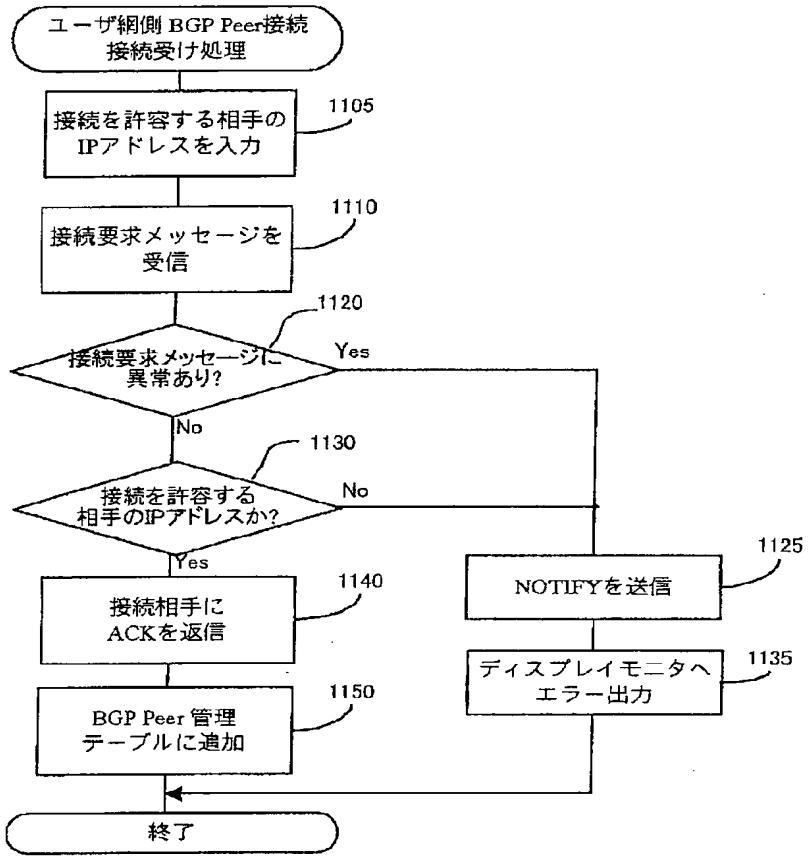
【図１０】

図10


ユーザ網側 BGP Peer接続
接続要求処理
Peer接続先の
IPアドレスを入力
1005
接続要求メッセージを
送信
1010
1020
接続相手から
NOTIFYを受信?
Yes
No
接続相手から
ACKを受信
1030
ディスプレイモニタへ
エラー出力
1025
BGP Peer 管理テーブル
に追加
1040
終了

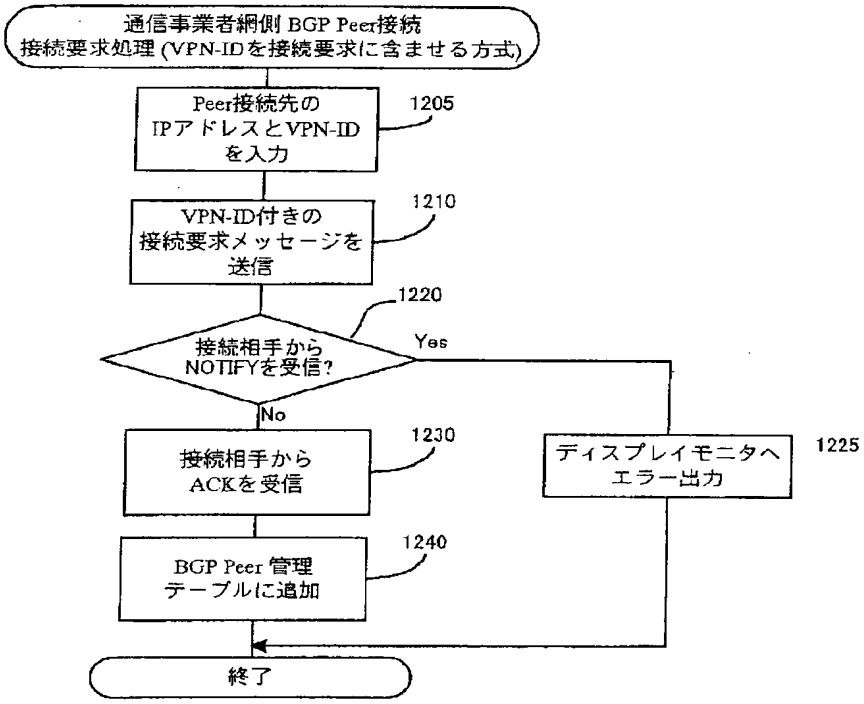
【図１１】

図11


ユーザ網側 BGP Peer接続
接続受け処理
接続を許容する相手の
IPアドレスを入力
1105
接続要求メッセージを
受信
1110
1120
接続要求メッセージに
異常あり?
Yes
No
1130
接続を許容する
相手のIPアドレスか?
No
Yes
接続相手に
ACKを返信
1140
BGP Peer 管理
テーブルに追加
1150
NOTIFYを送信
1125
ディスプレイモニタへ
エラー出力
1135
終了

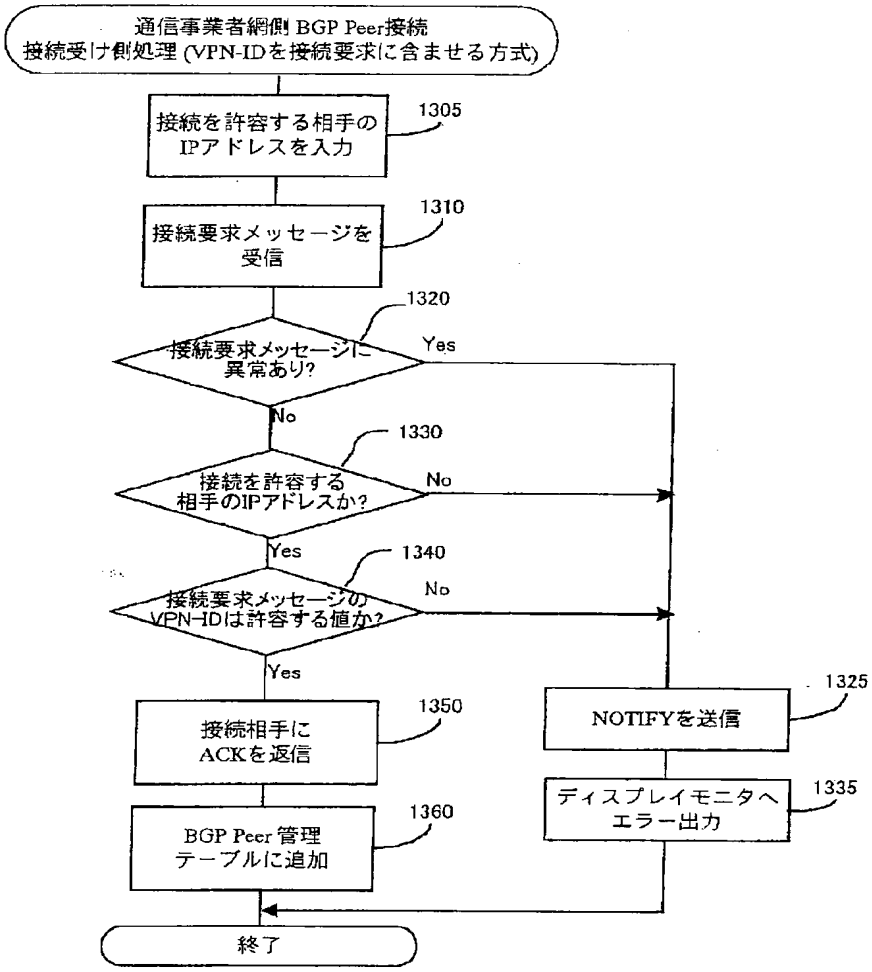
【図１２】

図12


通信事業者網側 BGP Peer接続
接続要求処理 (VPN-IDを接続要求に含ませる方式)
Peer接続先の
IPアドレスとVPN-ID
を入力
1205
VPN-ID付きの
接続要求メッセージを
送信
1210
1220
接続相手から
NOTIFYを受信?
Yes
No
接続相手から
ACKを受信
1230
ディスプレイモニタへ
エラー出力
1225
BGP Peer 管理
テーブルに追加
1240
終了

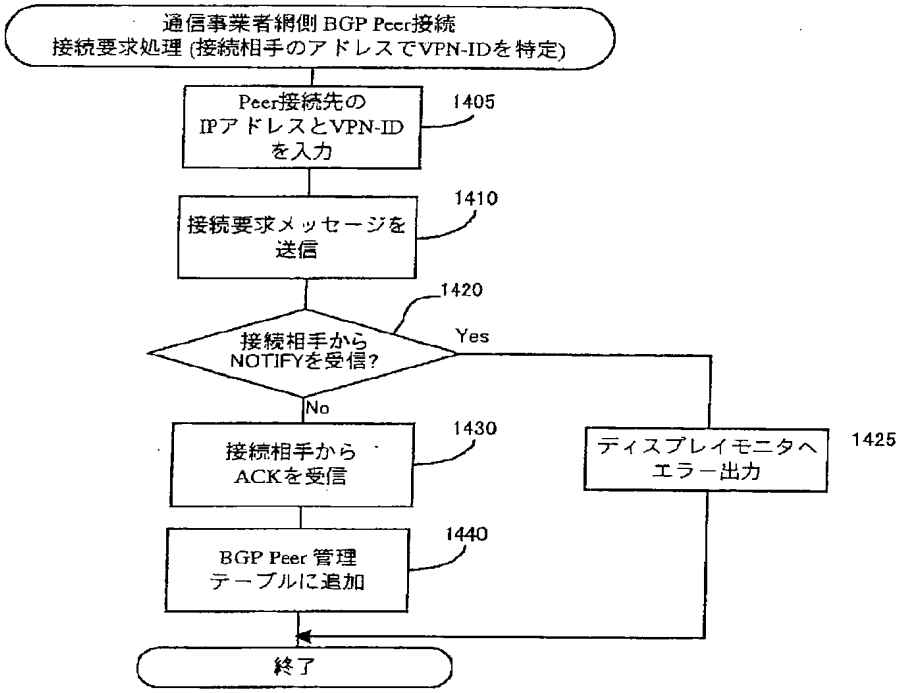
【図１３】

図13


通信事業者網側 BGP Peer接続
接続受け側処理 (VPN-IDを接続要求に含ませる方式)
接続を許容する相手の
IPアドレスを入力
1305
接続要求メッセージを
受信
1310
接続要求メッセージに
異常あり?
1320
Yes
No
接続を許容する
相手のIPアドレスか?
1330
No
Yes
接続要求メッセージの
VPN-IDは許容する値か?
1340
No
Yes
接続相手に
ACKを返信
1350
BGP Peer 管理
テーブルに追加
1360
NOTIFYを送信
1325
ディスプレイモニタへ
エラー出力
1335
終了

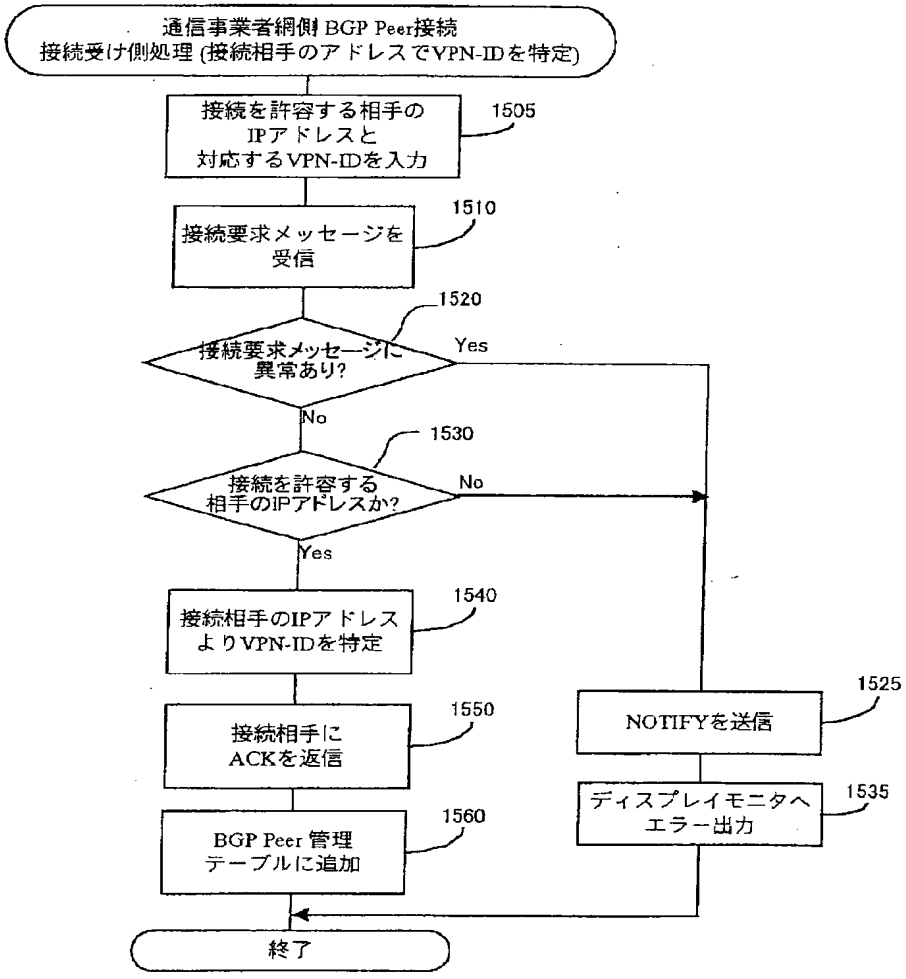
【図１４】

図14


通信事業者網側 BGP Peer接続
接続要求処理 (接続相手のアドレスでVPN-IDを特定)
Peer接続先の
IPアドレスとVPN-ID
を入力
1405
接続要求メッセージを
送信
1410
1420
接続相手から
NOTIFYを受信?
Yes
No
接続相手から
ACKを受信
1430
ディスプレイモニタへ
エラー出力
1425
BGP Peer 管理
テーブルに追加
1440
終了

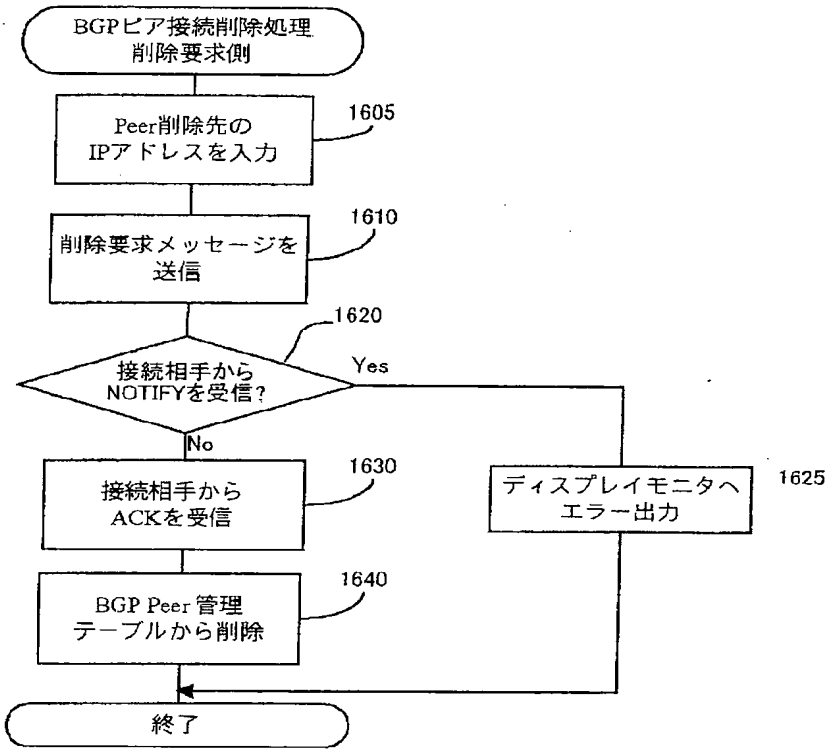
【図１５】

図15


通信事業者網側 BGP Peer接続
接続受け側処理 (接続相手のアドレスでVPN-IDを特定)
接続を許容する相手の
IPアドレスと
対応するVPN-IDを入力
1505
接続要求メッセージを
受信
1510
1520
接続要求メッセージに
異常あり?
Yes
No
1530
接続を許容する
相手のIPアドレスか?
No
Yes
接続相手のIPアドレス
よりVPN-IDを特定
1540
接続相手に
ACKを返信
1550
BGP Peer 管理
テーブルに追加
1560
NOTIFYを送信
1525
ディスプレイモニタへ
エラー出力
1535
終了

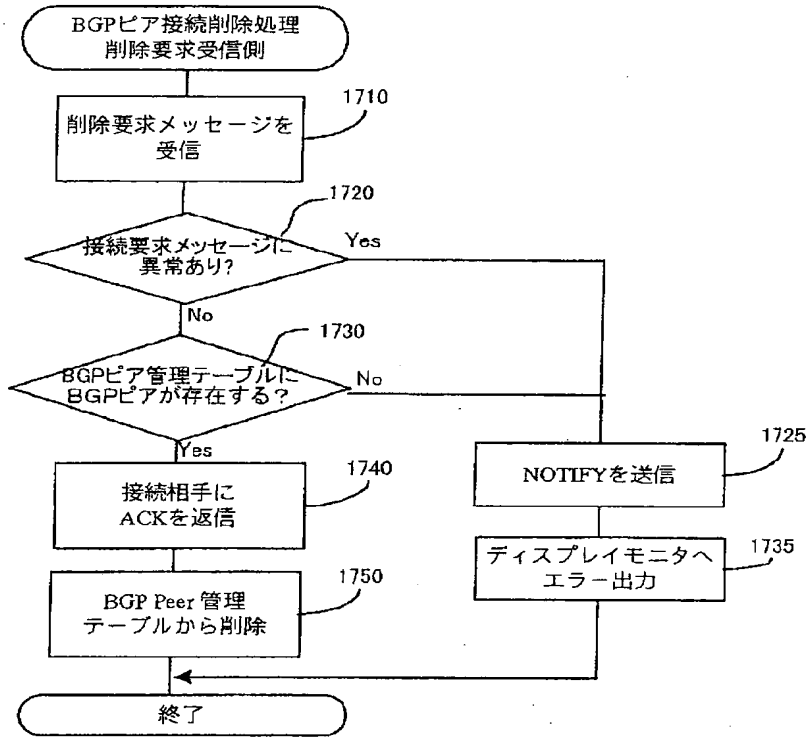
【図１６】

図16


BGPピア接続削除処理
削除要求側
Peer削除先の
IPアドレスを入力
1605
削除要求メッセージを
送信
1610
1620
接続相手から
NOTIFYを受信?
Yes
No
接続相手から
ACKを受信
1630
ディスプレイモニタへ
エラー出力
1625
BGP Peer管理
テーブルから削除
1640
終了

【図１７】

図17



フロントページの続き

(72)発明者　木本　淳志
神奈川県秦野市堀山下１番地　株式会社日立製作所エンタープライズサーバ事業部内

Ｆターム(参考)　5K030 HD03 KA05 LB02 LB05 LB19